

24+4G 千兆二层全网管交换机

TL-SL5428

命令行手册

Rev1.0.0

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目 录

手册概述

本手册提供 CLI（Command Line Interface,命令行界面）参考信息，适用于 TP-LINK TL-SL5428 24+4G 千兆二层全网管交换机。

各章节内容安排如下：

第 1 章：命令行使用指导

主要介绍 CLI 的使用方法、命令行模式、使用命令行、命令行分级及命令行格式约定。

第 2 章：用户界面

主要介绍用户登录和退出操作模式的相关配置命令。

第 3 章：IEEE 802.1Q VLAN 配置命令

主要介绍 IEEE 802.1Q VLAN 的相关配置命令。

第 4 章：MAC VLAN 配置命令

主要介绍 MAC-Based VLAN 的相关配置命令。

第 5 章：协议 VLAN 配置命令

主要介绍协议 VLAN 的相关配置命令。

第 6 章： VLAN-VPN 配置命令

主要介绍 VLAN-VPN 的相关配置命令。

第 7 章：语音 VLAN 的配置命令

主要介绍语音 VLAN 的相关配置命令。

第 8 章：GVRP 配置命令

主要介绍 GVRP 的相关配置命令。

第 9 章：端口汇聚配置命令

主要介绍端口汇聚的相关配置命令。

第 10 章：LACP 配置命令

主要介绍 LACP 相关配置命令。

第 11 章：用户管理配置命令

主要介绍用户管理信息的相关配置命令。

第 12 章：绑定列表配置命令

主要介绍 IP-MAC-VID-PORT 四元绑定表的相关配置命令。

第 13 章：ARP 防护配置命令

主要介绍防 ARP 欺骗、防 ARP 攻击、报文统计的相关配置命令。

第 14 章：IP 源防护配置命令

主要介绍 IP 源防护的相关配置命令。

第 15 章：DoS 防护命令

主要介绍 DoS 防护和攻击检测的相关配置命令。

第 16 章：IEEE 802.1X 配置命令

主要介绍 IEEE 802.1X 认证的相关配置命令。

第 17 章：系统日志配置命令

主要介绍系统日志的查看、输出，日志服务器的相关配置命令。

第 18 章：SSH 配置命令

主要介绍 SSH 配置管理的相关命令。

第 19 章：SSL 配置命令

主要介绍 SSL 配置管理的相关命令。

第 20 章：地址配置命令

主要介绍端口安全设置和地址表管理的相关配置命令。

第 21 章：系统配置命令

主要介绍系统信息、网络参数配置，系统软件复位，系统文件升级，交换机重启及连通性测试等系统相关配置命令。

第 22 章：以太网配置命令

主要介绍以太网端口的流量控制、协商模式、风暴抑制、带宽限制的相关配置命令。

第 23 章：QoS 配置命令

主要介绍 QoS（服务质量）的相关配置命令。

第 24 章：端口监控配置命令

主要介绍端口监控的相关配置命令。

第 25 章：ACL 配置命令

主要介绍访问控制的相关配置命令。

第 26 章：MSTP 配置命令

主要介绍生成树配置的相关配置命令。

第 27 章：IGMP 配置命令

主要介绍 IGMP 侦听、组播地址表管理、组播过滤等组播管理相关配置命令。

第 28 章：SNMP 配置命令

主要介绍 SNMP（简单网络管理协议）配置、通知管理、RMON（远程网络监视）等 SNMP 相关配置命令。

第 29 章：集群配置命令

主要介绍拓扑发现、拓扑收集、集群管理的相关配置命令。

第1章 命令行使用指导

1.1 使用命令行

用户可以通过两种方式登录交换机来使用命令行：

1. 通过 Console 口进行本地登录；
2. 通过以太网端口利用 Telnet 或 SSH 进行本地或远程登录。

1.1.1 通过 Console 口进行本地登录

1. 首先，将计算机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。
2. 选择**开始→ 所有程序→ 附件→ 通讯→ 超级终端**，打开超级终端。

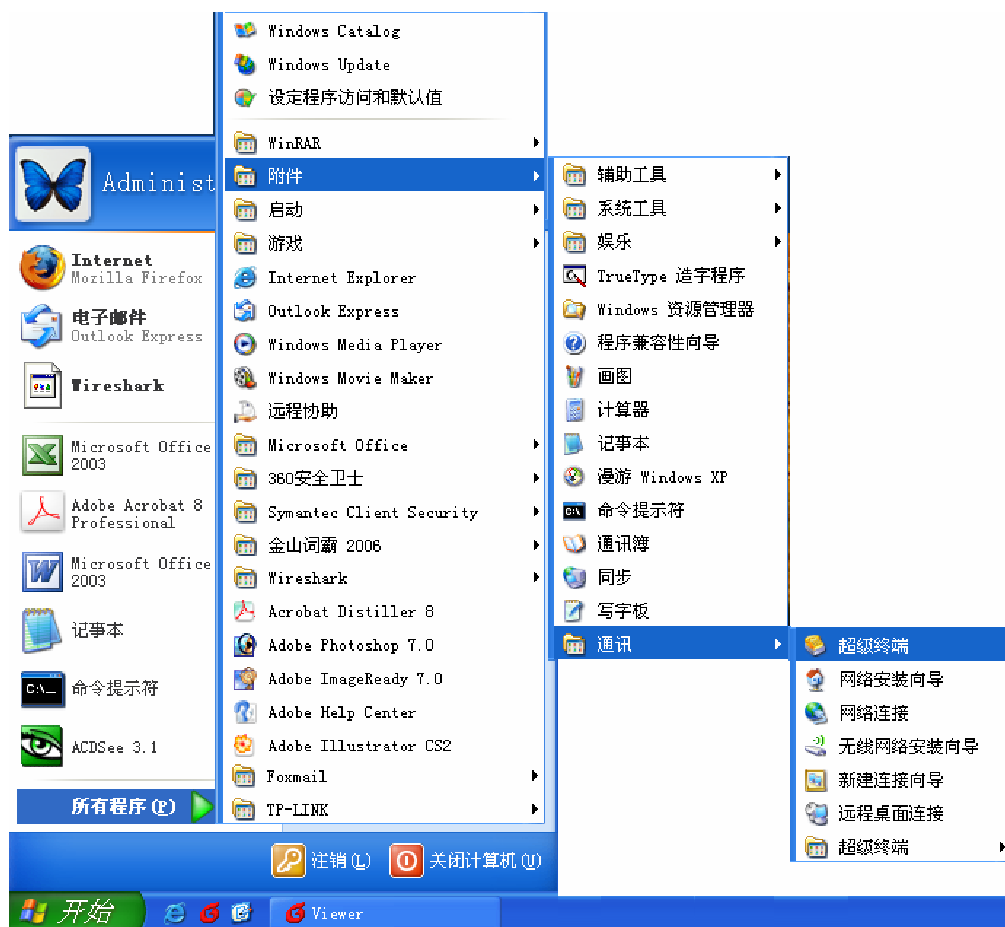


图 1-1 打开超级终端

3. 弹出如 图 1-2 所示的连接描述窗口，在名称处键入一个名称，点击**确定**。



图 1-2 连接描述

4. 在 图 1-3 中选择连接串口，点击**确定**。



图 1-3 连接端口选择

5. 在图 图 1-4 中对端口进行参数设置：每秒位数“38400”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，然后点击**确定**。

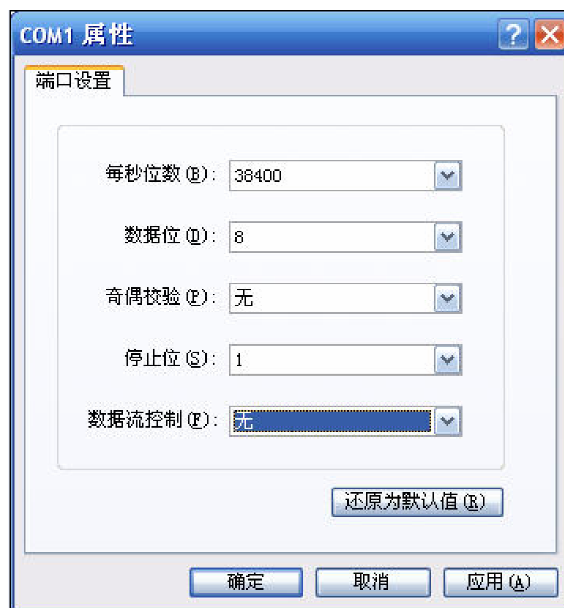


图 1-4 端口属性设置

6. 在超级终端主窗口中输入用户名和密码（默认值均为“admin”），按下回车键，可以看到“TP-LINK>”的提示符，说明已成功登录交换机。如 图 1-5 所示。

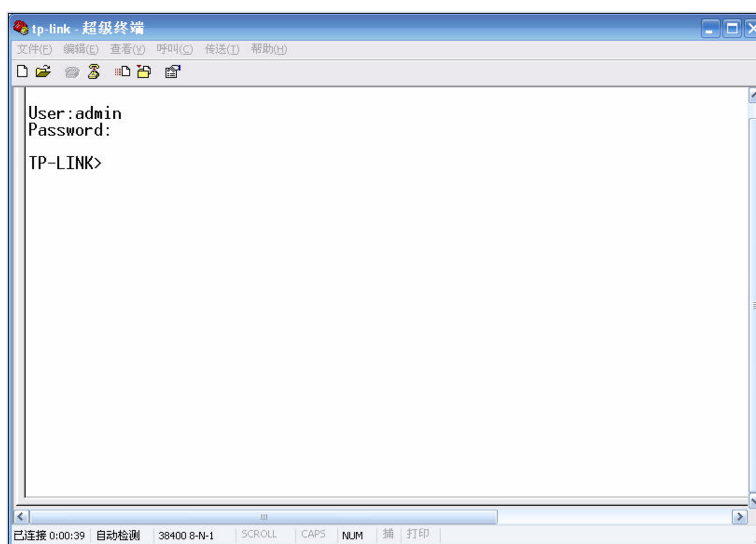


图 1-5 登录交换机

1.1.2 通过 Telnet 进行登录

1. 首先请确保本交换机与计算机在同一局域网内。

2. 选择**开始→运行**，打开运行窗口。



图 1-6 打开运行窗口

3. 弹出如 图 1-7 所示的运行窗口，输入cmd，点击**确定**按钮。

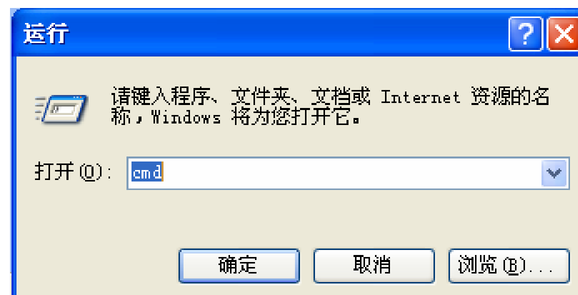


图 1-7 运行窗口

4. 在接下来的 图 1-8 命令提示符对话框中输入telnet 192.168.0.1，按下回车键。

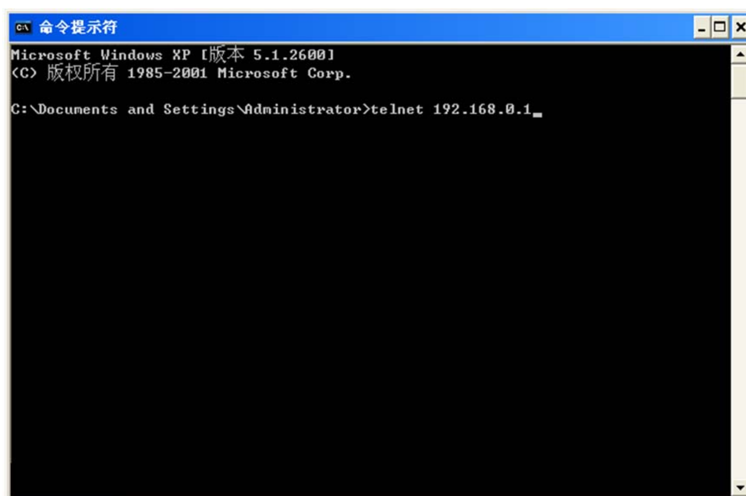


图 1-8 连接交换机

5. 输入登录的用户名和密码（默认值均为“admin”），回车即可登录，如 图 1-9。

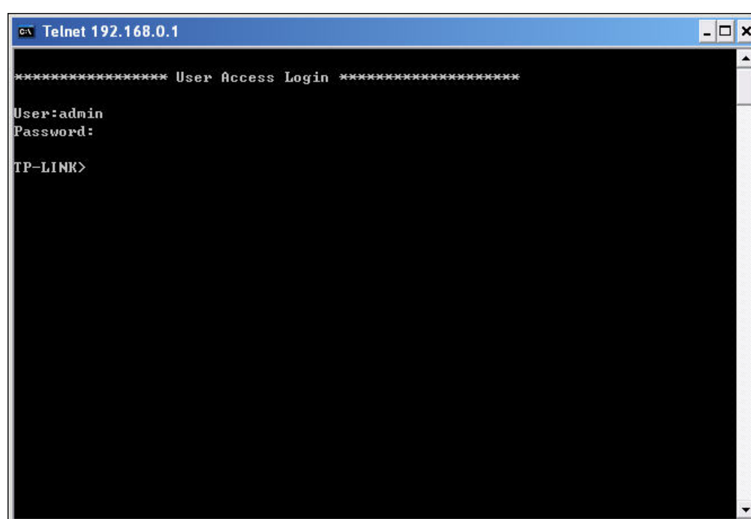
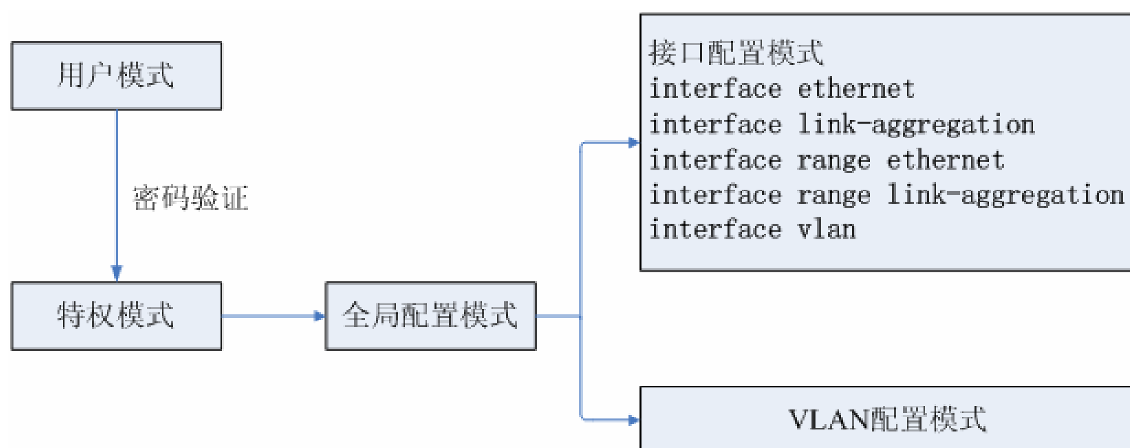


图 1-9 登录交换机

1.2 命令行模式

CLI 按功能划分为五种模式，即：用户模式、特权模式、全局配置模式、接口配置模式和 VLAN 配置模式，其中接口配置模式又分为以太网端口配置模式和汇聚端口配置模式等，如下图：



下表列出了各模式的访问方法、提示符以及如何离开各模式：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与交换机建立连接即进入该模式	**TP-LINK>**	输入**exit**命令断开与交换机连接（Console口接入时无法断开）； 输入**enable** 命令，进入特权模式。
特权模式	在用户模式下，使用**enable**命令进入该模式	**TP-LINK#**	输入**exit**命令断开与交换机连接（Console口接入时无法断开）； 输入**disable** 命令，返回用户模式； 输入**configure** 命令，进入全局配置模式。
全局配置模式	在特权模式下，使用**configure**命令进入该模式	**TP-LINK(config)#**	输入**exit** 命令或**end** 命令，或者键入Ctrl+Z组合键，返回特权模式； 输入**interface** *type number*命令，进入接口配置模式； 输入**vlan database**命令，进入VLAN 配置模式。
接口配置模式	在全局配置模式下键入**interface** *type number*进入该模式	**TP-LINK(config-if)#**	输入**end** 命令，或键入Ctrl+Z组合键，返回特权模式； 输入**exit**命令，返回全局配置模式； 在**interface** 命令中必须指明要进入哪一个接口配置子模式。
VLAN配置模式	在全局配置模式下，使用**vlan database**命令进入该模式	**TP-LINK(config-vlan)#**	输入**end** 命令，或键入Ctrl+Z组合键返回特权模式； 输入**exit** 命令，返回全局配置模式。

说明：

1. 通过Console口或Telnet方式与交换机建立连接后即进入用户模式。
2. 各个模式都有各自的命令，要进行相应的命令配置必须要先进入对应的模式：

- **全局配置模式**：提供全局配置的命令，如：生成树，队列调度模式等；
- **接口配置模式**：分为多个接口，每个接口都有各自相应的命令：
  a) interface ethernet：配置一个以太网端口的参数，如双工模式，流控状态等。
  b) interface range ethernet：包含的命令跟interface ethernet基本一样，配置多个以太网端口的参数。
  c) interface link-aggregation：配置汇聚端口的参数，广播风暴等。
  d) interface range link-aggregation：配置多个汇聚端口的参数。
  e) interface vlan：配置VLAN接口参数。
- **VLAN配置模式**：创建VLAN，增加端口到指定VLAN。

3. 有一些命令是全局的，在所有命令模式下都可执行：

- **show**：显示交换机各种信息，如：统计信息、端口信息、VLAN信息等。
- **history**：显示历史命令。

1.3 命令行安全等级

交换机主要分两个安全等级：参观级和管理级。

参观级只能在用户模式下进行简单的查询操作；管理级能在特权模式、全局配置模式、接口配置模式、VLAN 配置模式下对交换机进行监控、配置、管理等操作。

通过 Telnet 或 Console 方式登录时，输入正确的用户名和密码后将进入用户模式，即获得参观级权限。不过当用户类型为受限用户时，则不允许登录访问命令行。

在用户模式下，可通过输入命令 **enable** 来进入特权模式。使用 **enable** 命令进入特权模式时缺省情况下无密码，可以在全局配置模式下通过 **enable password** 命令设置管理级密码。无密码情况下键入 **enable** 命令直接进入特权模式，有密码情况下输入管理级密码才能进入特权模式。进入特权模式即获得管理级权限。

1.4 命令行格式约定

1.4.1 基本格式约定

本文档中对 CLI 命令的叙述遵循以下约定：

- 在中括号 [ ] 中的任何参数都是可选的。
- 在大括号 { } 中的任何参数都是必需的。
- 如果有多个选项，则使用竖线 "|"分隔每个选项。

  例如：**speed** { 10 | 100 | 1000 }
- 关键词（命令中保持不变，必须照输的部分）以粗体形式出现。

例如：**show logging**

- 常量（枚举量，只能选择其一）以普通字体形式出现。

  例如：**switchport type** { access | trunk | general }

- 变量（命令中必须以实际值进行替代的部分）以斜体形式出现。

  例如：**bridge aging-time** *aging-time*

1.4.2 特殊字符

若变量为字符串形式，输入时请注意：

- ” < > , \ & 这六个字符是不允许输入的。
- 若字符串中包含空格，则字符串首尾需添加单引号’’或双引号””，如’hello world’、”hello world”。此时单/双引号中的两个（或多个）单词会作为一个字符串参数输入；如果不加单/双引号，它们会被解析成两个（或多个）字符串。

1.4.3 参数格式

变量中有些参数是有特定的输入格式的：

- MAC 地址必须以 XX:XX:XX:XX:XX:XX 的格式输入。
- 输入一组端口号(port-list)或一组 VLAN 号(vlan-list)时，输入格式为 1,3-5,7，即可以输入一个或多个值，每个值之间用逗号隔开；连续的一组值可以用连接符-表示。

第2章 用户界面

2.1 enable

该命令用于从用户模式进入特权模式。

命令

enable

模式

用户模式

示例

设置了从用户模式进入特权模式的密码时：

```
TP-LINK>enable
Enter password:
TP-LINK#
```

2.2 enable password

该命令用于设置从用户模式切换到特权模式的管理级密码，它的 no 命令用于清空密码。

命令

enable password *password*

no enable password

参数

password —— 管理级密码，由 1~16 个字符（只能为数字、字母和下划线）组成，默认为空。

模式

全局配置模式

示例

将用户模式切换到特权模式时的管理级密码设置为 admin：

```
TP-LINK(config)# enable password admin
```

2.3 disable

该命令用于从特权模式返回到用户模式。

命令

disable

模式

特权模式

示例

从特权模式返回到用户模式：

```
TP-LINK# disable
TP-LINK>
```

2.4 configure

该命令用于从特权模式进入全局配置模式。

命令

configure

模式

特权模式

示例

从特权模式进入全局配置模式：

```
TP-LINK# configure
TP-LINK(config)#
```

2.5 exit

该命令用于退出当前配置模式返回上一层配置模式。

命令

exit

模式

所有配置模式

示例

从接口配置模式返回到全局模式，再返回到特权模式：

```
TP-LINK(config-if)# exit
TP-LINK(config)#exit
TP-LINK#
```

2.6 end

该命令用于返回特权模式。

命令

end

模式

所有配置模式

示例

从接口配置模式直接返回到特权模式：

```
TP-LINK(config-if)#end
TP-LINK#
```

第3章 IEEE 802.1Q VLAN配置命令

VLAN（Virtual Local Area Network，虚拟局域网）是一种在一个物理网络上划分多个逻辑网络的技术，具有控制广播域范围，增强网络安全性，可以灵活创建虚拟工作组等优点。

3.1 vlan database

该命令用于进入 VLAN 配置模式下进行创建、删除 IEEE 802.1Q VLAN 等操作。

命令

vlan database

模式

全局配置模式

示例

进入 VLAN 配置模式：

```
TP-LINK(config)# vlan database
TP-LINK(config-vlan)#
```

3.2 vlan

该命令用于用于创建 IEEE 802.1Q VLAN，它的 no 命令用于删除 IEEE 802.1Q VLAN。

命令

vlan *vlan-id*

no vlan *vlan-id*

参数

vlan-id —— VLAN ID，取值范围 2~4094。

模式

VLAN 配置模式

示例

创建 vid=12 的 vlan：

```
TP-LINK(config)# vlan database
TP-LINK(config-vlan)#vlan 12
```

3.3 interface vlan

该命令用于进入 VLAN 接口模式对指定 VLAN 进行配置。

命令

interface vlan *vlan-id*

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

全局配置模式

示例

对 vid=2 的 VLAN 进行配置：

TP-LINK(config)# interface vlan 2

3.4 description

该命令用于配置 IEEE 802.1Q VLAN 描述字符，它的 no 命令用于清空描述字符。

命令

description *descript*

no descriotion

参数

descript —— VLAN 描述字符，长度为 1-16 个字符。

模式

接口配置模式（interface vlan）

示例

将 vid=2 的 VLAN 描述成”vlan2”：

TP-LINK(config)# interface vlan 2

TP-LINK(config-if)#description vlan2

3.5 switchport type

该命令用于配置以太网端口的链路类型。

命令

switchport type { access | trunk | general }

参数

access | trunk | general —— 以太网端口链路类型，共支持三种类型。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

配置太网端口 5 的链路类型为 general：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)#switchport type general

3.6 switchport allowed vlan

该命令用于把指定端口添加到 IEEE 802.1Q VLAN，或把端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport allowed vlan add *vlan-list*

switchport allowed vlan remove *vlan-list*

参数

vlan-list —— VLAN ID 列表，可将端口加入到多个 VLAN 或从多个 VLAN 中移除。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将以太网端口 2 添加到 VLAN2 中：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# switchport allowed vlan add 2

3.7 switchport pvid

该命令用于设置交换机端口的 PVID。

命令

switchport pvid vlan-id

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置端口 2 的 PVID 为 2：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# switchport pvid 2

3.8 switchport general egress-rule

该命令用于配置 general 类型端口的出口规则（egress-rule）。

命令

switchport general egress-rule { untagged | tagged }

参数

untagged | tagged —— 出口规则，untagged 或者 tagged

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 2 的出口规则配置为 tagged：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# switchport general egress-rule tagged

3.9 show vlan

该命令用于显示 IEEE 802.1Q VLAN 信息。

命令

show vlan [*vlan-id*]

参数

vlan-id —— VLAN ID，取值范围为 1-4094。该参数缺省时，显示所有 IEEE 802.1Q VLAN 的信息。

模式

所有命令模式

示例

显示 vid=5 的 IEEE 802.1Q VLAN 信息：

TP-LINK(config)# show vlan 5

3.10 show interface switchport

该命令用于显示特定端口的 IEEE 802.1Q VLAN 配置信息。

命令

show interface switchport [*port-num*]

参数

port-num —— 端口号。该参数缺省时，显示所有端口的 VLAN 配置信息。

模式

所有命令模式

示例

显示所有端口的 VLAN 配置信息：

```
TP-LINK(config)# show interface switchport
```

第4章 MAC VLAN配置命令

MAC VLAN 功能是按照 MAC 地址来来划分 VLAN 的一种方法。每个 MAC 地址对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。

4.1 mac-vlan add

该命令用于创建 MAC-Based VLAN 条目。

命令

mac-vlan add {*vlan-id*} {*mac-addr*} [*description*]

参数

vlan-id —— 选择 VLAN ID，取值范围 1-4094。

mac-addr —— 源 MAC 地址。

description —— 对该 MAC VLAN 条目的描述。该参数缺省时，描述字符为空。

模式

全局配置模式

示例

创建 vid=2，MAC 地址为 00:00:00:00:00:01 的 MAC-Based VLAN 条目：

TP-LINK(config)# mac-vlan add 2 00:00:00:00:00:01 RD

4.2 mac-vlan remove

该命令用于删除已存在的 MAC-Based VLAN 条目。

命令

mac-vlan remove {*mac-addr*}

参数

mac-addr —— 源 MAC 地址。

模式

全局配置模式

示例

删除一条 MAC VLAN 条目（假设 MAC 为 00:00:00:00:00:02）：

TP-LINK(config)# mac-vlan remove 00:00:00:00:00:02

4.3 mac-vlan modify

该命令用于修改已存在的 MAC VLAN 条目。

命令

mac-vlan modify {*vlan-id*} {*mac-addr*} [*description*]

参数

vlan-id —— 选择 VLAN ID，取值范围 1-4094。

mac-addr —— 源 MAC 地址。

description —— 对该 MAC VLAN 条目的描述。该参数缺省时，对原描述不作修改。

模式

全局配置模式

示例

修改一条 MAC VLAN 条目（假设 MAC 为 00:00:00:00:00:02），将其对应的 VLAN ID 修改为 12：

TP-LINK(config)# mac-vlan modify 12 00:00:00:00:00:02

4.4 mac-vlan interface

该命令用于启用指定端口的 MAC VLAN 功能，它的 no 命令用于禁用指定端口的 MAC VLAN 功能，缺省时在所有端口上禁用 MAC VLAN 功能。

命令

mac-vlan interface *port-list*

no mac-vlan interface [*port-lsit*]

参数

port-list —— 端口列表，对列表中的端口进行配置或取消配置。

模式

全局配置模式

示例

开启端口 1-3，11-15 的 MAC VLAN 功能：

TP-LINK(config)# mac-vlan interface 1-3,11-15

4.5 show mac-vlan

该命令用于显示 MAC VLAN 条目信息。

命令

show mac-vlan

模式

所有命令模式

示例

显示 MAC VLAN 条目信息：

```
TP-LINK(config)# show mac-vlan
```

4.6 show mac-vlan interface

该命令用于显示 MAC VLAN 的端口使能状态。

命令

show mac-vlan interface

模式

所有命令模式

示例

显示 MAC VLAN 的端口使能状态：

```
TP-LINK(config)# show mac-vlan interface
```

第5章　协议VLAN配置命令

协议 VLAN 是按照协议来划分 VLAN 的一种方法。每个协议对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。

5.1 protocol-vlan template

该命令用于创建或删除 Protocol VLAN 协议模板。

命令

protocol-vlan template add {*protocol-name*} {*ether-type*}

protocol-vlan template remove *index*

参数

protocol-name —— 协议名称，由 1-8 个字符组成。

ether-type —— 协议类型，由 4 位十六进制数组成。

index —— 协议模板序号。可用 **show protocol-vlan template** 命令获取各序号对应的模板。

模式

全局配置模式

示例

创建协议类型为 0806 的 arp 协议模板，并删除 2 号协议模板：

TP-LINK(config)# protocol-vlan template add arp 0806

TP-LINK(config)# protocol-vlan template remove 2

5.2 protocol-vlan vlan

该命令用于创建 Protocol VLAN 条目，它的 no 命令则用于删除 Protocol VLAN 条目。

命令

protocol-vlan vlan *vid* **template** *index*

no protocol-vlan *entry-id*

参数

vid ——VLAN ID，取值范围 1-4094。

index ——协议模板序号。可用 **show protocol-vlan template** 命令获取各序号对应的模板。

entry-id ——协议 VLAN 序号。可用 **show protocol-vlan vlan** 命令获取各序号对应的协议 VLAN 条目。

模式

全局配置模式

示例

创建 vid=2，协议模板序号为 1 的 Protocol VLAN 条目；并删除序号为 1 的 Protocol VLAN 条目：

TP-LINK(config)# protocol-vlan vlan 2 **template** 1

TP-LINK(config)# no protocol-vlan vlan 1

5.3 protocol-vlan interface

该命令用于在指定端口上启用 Protocol VLAN 属性，它的 no 命令用于禁用指定端口的 Protocol VLAN 属性，缺省时在所有端口上禁用 Protocol VLAN 属性。

命令

protocol-vlan vlan interface *port-list*

no protocol-vlan interface [*port-list*]

参数

port-list ——端口列表，对列表中的端口进行配置或取消配置。

模式

全局配置模式

示例

启用端口 1、4-6、9-11 的 Protocol VLAN 属性：

TP-LINK(config)# protocol-vlan vlan interface 1,4-6,9-11

5.4 show protocol-vlan template

该命令用于显示 Protocol VLAN 协议模块配置信息。

命令

show protocol-vlan template

模式

所有命令模式

示例

显示 Protocol VLAN 协议模板配置信息：

```
TP-LINK(config)# show protocol-vlan template
```

5.5 show protocol-vlan vlan

该命令用于显示 Protocol VLAN 条目信息。

命令

show protocol-vlan vlan

模式

所有命令模式

示例

显示 Protocol VLAN 条目信息：

```
TP-LINK(config)# show protocol-vlan vlan
```

5.6 show protocol-vlan interface

该命令用于显示 Protocol VLAN 端口配置信息。

命令

show protocol-vlan interface

模式

所有命令模式

示例

显示 Protocol VLAN 端口配置信息：

```
TP-LINK(config)# show protocol-vlan interface
```

第6章 VLAN-VPN配置命令

VLAN-VPN(Virtual Private Network)是一种简单、灵活的二层 VPN 技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商网络（公网）。

6.1 vlan-vpn enable

该命令用于全局启用 VLAN-VPN 功能，它的 no 命令用于禁用 VLAN-VPN 功能。

命令

vlan-vpn enable

no vlan-vpn enable

模式

全局配置模式

示例

全局启用 VLAN-VPN 功能：

TP-LINK(config)# vlan-vpn enable

6.2 vlan-vpn tpid

该命令用于配置 VLAN-VPN 全局 TPID，它的 no 命令用于恢复默认 TPID。

命令

vlan-vpn tpid *tpid*

no vlan-vpn tpid

参数

tpid —— 全局 TPID。必须为 4 位十六进制整数的形式。默认值为 8100。

模式

全局配置模式

示例

配置 VLAN-VPN 全局 TPID 为 8200：

TP-LINK(config)# vlan-vpn tpid 8200

6.3 vlan-vpn vlan-mapping add

该命令用于添加 VLAN 映射条目。

命令

vlan-vpn vlan-mapping add *c-vlan sp-vlan* [*description*]

参数

c-vlan —— Customer VLAN ID（用户 VLAN ID），取值范围 1-4094。

sp-vlan —— Service Provider VLAN ID（服务商 VLAN ID），取值范围 1-4094。

description —— VLAN 映射条目的附加信息，可选。

模式

全局配置模式

示例

添加一条 VLAN 映射条目，C-VLAN 为 2，SP-VLAN 为 200：

TP-LINK(config)# vlan-vpn vlan-mapping add 2 200

6.4 vlan-vpn vlan-mapping modify

该命令用于修改已存在的 VLAN 映射条目。

命令

vlan-vpn vlan-mapping modify *c-vlan sp-vlan* [*description*]

参数

c-vlan ——用户 VLAN ID（Customer VLAN ID），取值范围 1-4094。

sp-vlan ——服务商 VLAN ID（Service Provider VLAN ID），取值范围 1-4094。

description —— VLAN 映射条目的附加信息，可选。

模式

全局配置模式

示例

修改一条已存在 VLAN 映射条目（假设 C-VLAN 为 2），将 SP-VLAN 重设为 100：

TP-LINK(config)# vlan-vpn vlan-mapping modify 2 100

6.5 vlan-vpn vlan-mapping remove

该命令用于删除已存在的 VLAN 映射条目（根据 C-VLAN ID）。

命令

vlan-vpn vlan-mapping remove *c-vlan*

参数

c-vlan —— Customer VLAN ID（用户 VLAN ID），取值范围 1-4094。

模式

全局配置模式

示例

删除一条已存在 VLAN 映射条目（假设 C-VLAN 为 2）：

TP-LINK(config)# vlan-vpn vlan-mapping remove 2

6.6 vlan-vpn vlan-mapping interface

该命令用于启用指定端口的 VLAN 映射功能，它的 no 命令用于禁用指定端口的 VLAN 映射功能，缺省时在所有端口上禁用 VLAN 映射功能。

命令

vlan-vpn vlan-mapping interface *port-list*

no vlan-vpn vlan-mapping [*port-list*]

参数

port-list ——端口列表，对列表中的端口进行配置或取消配置。

模式

全局配置模式

示例

开启端口 2-5、16-18 的 VLAN 映射功能：

TP-LINK(config)# vlan-vpn vlan-mapping interface 2-5,16-18

6.7 vlan-vpn uplink

该命令用于配置指定端口为上联端口，它的 no 命令用于取消指定端口为上联端口，缺省时取消所有端口为上联端口。

命令

vlan-vpn uplink *port-list*

no vlan-vpn uplink [*port-list*]

参数

port-list —— 端口列表，对列表中的端口进行配置或取消配置。

模式

全局配置模式

示例

配置端口 1、3-5、8-10 为上联端口：

TP-LINK(config)# vlan-vpn uplink 1,3-5,8-10

6.8 show vlan-vpn global

该命令用于显示 VLAN VPN 全局配置信息。

命令

show vlan-vpn global

模式

所有命令模式

示例

显示 VLAN VPN 全局配置信息：

```
TP-LINK(config)# show vlan-vpn global
```

6.9 show vlan-vpn uplink

该命令用于显示 VLAN VPN 上联端口配置信息。

命令

show vlan-vpn uplink

模式

所有命令模式

示例

显示 VLAN VPN 上联端口配置信息：

```
TP-LINK(config)# show vlan-vpn uplink
```

6.10 show vlan-vpn vlan-mapping

该命令用于显示 VLAN 映射条目信息。

命令

show vlan-vpn vlan-mapping

模式

所有命令模式

示例

显示 VLAN 映射条目信息：

```
TP-LINK(config)# show vlan-vpn vlan-mapping
```

6.11 show vlan-vpn vlan-mapping interface

该命令用于显示 VLAN 映射的端口使能状态。

命令

show vlan-vpn vlan-mapping interface

模式

所有命令模式

示例

显示 VLAN 映射的端口使能状态：

```
TP-LINK(config)# show vlan-vpn vlan-mapping interface
```

第7章　语音VLAN配置命令

语音 VLAN 是为语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据流配置 QoS 参数，提高语音数据流的传输优先级、保证通话质量。

7.1 voice-vlan enable

该命令用于开启 Voice VLAN 功能，它的 no 命令用于禁用 Voice VLAN 功能。

命令

voice-vlan enable *vlan-id*

no voice-vlan enable

参数

vlan-id —— VLAN ID，取值范围 2-4094。

模式

全局配置模式

示例

开启 vid=2 的 Voice VLAN 功能：

```
TP-LINK(config)# voice-vlan enable 2
```

7.2 voice-vlan aging-time

该命令用于配置 Voice VLAN 老化时间，它的 no 命令用于恢复默认老化时间。

命令

voice-vlan aging-time *aging-time*

no voice-vlan aging-time

参数

aging-time —— 老化时间，取值范围 1-43200 (minutes)。默认值为 1440。

模式

全局配置模式

示例

配置 Voice VLAN 老化时间为 2880minutes：

```
TP-LINK(config)# voice-vlan aging-time 2880
```

7.3 voice-vlan priority

该命令用于配置 Voice VLAN 优先级，它的 no 命令用于恢复默认优先级。

命令

voice-vlan priority *priority*

no voice-vlan priority

参数

priority ——优先级，取值范围 0-6。默认值为 6。

模式

全局配置模式

示例

将 Voice VLAN 优先级配置为 3：

TP-LINK(config)# voice-vlan priority 3

7.4 voice-vlan oui

该命令用于创建或删除 Voice VLAN OUI 。

命令

voice-vlan oui add *mac-addr* **mask** *mask-addr* [*description*]

voice-vlan oui remove *mac-addr*

参数

mac-addr —— OUI 设备 MAC 地址。

mask-addr —— MAC 地址掩码。

description —— OUI 描述，1-16 个字符。缺省情况下为空。

模式

全局配置模式

示例

创建 MAC 地址为 00:01:E3:00:00:01，掩码为 FF:FF:FF:00:00:00 的 Voice VLAN OUI，将其描述为 TP-LINK Phone；并删除 MAC 地址为 00:00:00:11:00:01 的 Voice VLAN OUI：

TP-LINK(config)# voice-vlan oui add 00:01:E3:00:00:01 **mask** FF:FF:FF:00:00:00 “TP-LINK Phone“

TP-LINK(config)# voice-vlan oui remove 00:00:00:11:00:01

7.5 switchport voice-vlan mode

该命令用于配置以太网端口的 Voice VLAN 成员模式。

命令

switchport voice-vlan mode { manual | auto }

参数

manual / auto —— 端口的成员模式。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

配置以太网端口 2 的 voice vlan 成员模式为 manual：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# switchport voice-vlan mode manual

7.6 switchport voice-vlan security

该命令用于配置以太网端口的 Voice VLAN 安全模式。

命令

switchport voice-vlan security {disable | enable}

参数

disable / enable —— 禁用/启用指定端口的安全模式。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用以太网端口 2 的 Voice VLAN 安全模式：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# switchport voice-vlan security enable

7.7 show voice-vlan global

该命令用于显示 Voice VLAN 全局配置。

命令

show voice-vlan global

模式

所有命令模式

示例

显示 voice VLAN 全局配置信息：

TP-LINK(config)# show voice-vlan global

7.8 show voice-vlan oui

该命令用于显示 Voice VLAN OUI 配置信息。

命令

show voice-vlan oui

模式

所有命令模式

示例

显示 voice VLAN OUI 配置信息：

TP-LINK(config)# show voice-vlan oui

7.9 show voice-vlan switchport

该命令用于显示以太网端口的 Voice VLAN 配置信息。

命令

show voice-vlan switchport [*port*]

参数

port —— 以太网端口。该参数缺省时，显示所有端口的配置信息。

模式

所有命令模式

示例

显示所有端口的配置信息：

TP-LINK(config)# show voice-vlan switchport

第8章 GVRP配置命令

GARP（Generic Attribute Registration Protocol,通用属性注册协议），GVRP 功能是该协议的一种应用，通过在端口动态注册和注销 VLAN 信息来达到创建或删除 VLAN 的目的，并传播该信息到其它交换机中，减少配置 VLAN 时烦琐的手动操作。

8.1 gvrp

该命令用于全局启用 GVRP 功能，它的 no 命令用于禁用 GVRP 功能。

命令

gvrp

no gvrp

模式

全局配置模式

示例

全局启用 GVRP 功能：

```
TP-LINK(config)# gvrp
```

8.2 gvrp (interface)

该命令用于在指定端口上启用 GVRP 功能，它的 no 命令用于禁用该端口的 GVRP 功能。

命令

gvrp

no gvrp

模式

接口配置模式（interface ethernet / interface range ehternet）

说明

类型为 trunk 的端口才能启用 GVRP 功能。

示例

启用端口 2-6 的 GVRP 功能：

```
TP-LINK(config)# interface range ethernet 2-6
TP-LINK(config-if)# gvrp
```

8.3 gvrp registration

该命令用于配置指定端口的 GVRP 注册模式，它的 no 命令用于恢复默认的注册模式。

命令

gvrp registration { normal | fixed | forbidden }

no gvrp registration

参数

normal | fixed | forbidden —— 注册模式，默认的为 normal。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

配置端口 2-6 的 GVRP 注册模式为 fixed：

TP-LINK(config)# interface range ethernet 2-6

TP-LINK(config-if)# gvrp registration fixed

8.4 gvrp timer

该命令用于配置 GVRP 定时器，它的 no 命令用于恢复默认配置。

命令

gvrp timer { leaveall | join | leave } {*value*}

no gvrp timer [leaveall | join | leave]

参数

leaveall | join | leave —— 分别表示 leave All、join 和 leave 三个定时器。每个端口启动 GARP 后，同时启动 LeaveAll 定时器，端口将对外循环发送 LeaveAll 消息，以使其它端口重新注册其所有的属性信息。GARP 端口可以将每个 Join 数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用 Join 定时器来控制。接收到 Leave 数据包的 GARP 端口启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 数据包，则注销相应属性信息。

value —— 定时器值，leave All 的取值范围 1000-30000，默认值为 1000；join 的取值范围 20-1000，默认值为 20；leave 的取值范围 60-3000，默认值为 60。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 6 的 leaveall 定时器设为 2000，并将 join 定时器恢复默认配置：

```
TP-LINK(config)# interface ethernet 6
TP-LINK(config-if)# gvrp timer leaveall 2000
TP-LINK(config-if)# no gvrp timer join
```

8.5 show gvrp global

该命令用于显示 GVRP 全局状态。

命令

show gvrp global

模式

所有命令模式

示例

显示 GVRP 全局状态：

```
TP-LINK(config)# show gvrp global
```

8.6 show gvrp interface

该命令用于显示以太网端口的 GVRP 配置信息。

命令

show gvrp interface [**ethernet** *port-num*]

参数

port-num —— 以太网端口号，缺省时显示所有端口的 GVRP 配置信息。

模式

所有命令模式

示例

显示所有端口的 GVRP 配置信息：

```
TP-LINK(config)# show gvrp interface
```

第9章　端口汇聚配置命令

LAG(Link Aggregation Group,端口汇聚组)是将交换机的多个物理端口汇聚成一个逻辑端口的功能，可以增加带宽，提高连接的可靠性。

9.1 interface link-aggregation

该命令用于进入端口汇聚接口模式，它的 no 命令用于删除该汇聚组。

命令

interface link-aggregation *group-number*

no Interface link-aggregation *group-number*

参数

group-number —— 汇聚组，取值范围 1-14，最多可配置 14 个汇聚组。

模式

全局配置模式

示例

进入端口汇聚模式，对 group-number=1 的汇聚组进行配置：

TP-LINK(config)# interface link-aggregation 1

TP-LINK(config-if)#

9.2 interface range link-aggregation

该命令用于进入端口汇聚接口模式，同时配置多个端口汇聚组，它的 no 命令用于删除相应的汇聚组。

命令

interface range link-aggregation *group-list*

no interface range link-aggregation *group-list*

模式

全局配置模式

参数

group-list ——汇聚组列表，可指定多个汇聚组。

示例

进入端口汇聚接口模式并对汇聚组 1，4-6 进行配置：

TP-LINK(config)# interface range link-aggregation 1,4-6

```
TP-LINK(config-if)#
```

9.3 link-aggregation

该命令用于把端口添加到汇聚组，它的 no 命令用于将端口从汇聚组中移除。

命令

link-aggregation *group-num*

no link-aggregation

参数

group-num —— 汇聚组，取值范围 1-14。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 2-4 添加到汇聚组 1：

```
TP-LINK(config)# interface range ethernet 2-4
TP-LINK(config-if)#link-aggregation 1
```

9.4 link-aggregation hash-algorithm

该命令用于选择端口汇聚的选路算法。

命令

link-aggregation hash-algorithm {*src_dst_mac* | *src_dst_ip* }

参数

src_dst_mac —— 源目的 MAC 地址。

src_dst_ip —— 源目的 IP 地址。

模式

全局配置模式

示例

选择端口汇聚的选路算法为 src_dst_mac：

```
TP-LINK(config)# link-aggregation hash-algorithm src_dst_mac
```

9.5 description

该命令用于配置端口汇聚组的描述。它的 no 命令用于将描述字符清除。

命令

description *description*

no description

参数

description—— 汇聚组描述，1-16 个字符。

模式

接口配置模式（interface link-aggregation）

示例

将端口汇聚组 1 的描述配置为 movie server：

TP-LINK(config)# interface link-aggregation 1

TP-LINK(config-if)# description “movie server”

9.6 show interfaces link-aggregation

该命令用于显示全局选路算法和各汇聚组的配置情况。

命令

show interface link-aggregation [*group-num*]

参数

group-num —— 汇聚组，取值范围 1-14。该参数缺省时显示所有汇聚组的配置信息。

模式

所有命令模式

示例

显示所有汇聚组的配置信息：

TP-LINK(config)#show interface link-aggregation

第10章 LACP配置命令

LACP（Link Aggregation Control Protocol,链路汇聚控制协议）是基于 IEEE 802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。聚合的双方通过协议交互聚合信息，将匹配的链路聚合在一起收发数据，具有很高的灵活性并提供了负载均衡的能力。

10.1 lacp

该命令用于全局启用 LACP 功能，它的 no 命令用于禁用 LACP 功能。

命令

lacp

no lacp

模式

全局配置模式

示例

全局启用 LACP 功能：

```
TP-LINK(config)# lacp
```

10.2 lacp (interface)

该命令用于启用端口的 LACP 特性，它的 no 命令用于禁用端口的 LACP 特性。

命令

lacp

no lacp

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 1 的 LACP 特性：

```
TP-LINK(config)# interface ethernet 1
TP-LINK(config-if)# lacp
```

10.3 lacp admin-key

该命令用于配置端口的管理 Key，它的 no 命令用于恢复默认值。

命令

lacp admin-key *value*

no lacp admin-key

参数

value —— 管理 Key 值，取值范围 0-65535。默认值为 0。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置端口 1 的管理 Key 为 1024：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# lacp admin-key 1024

10.4 lacp system-priority

该命令用于配置端口的系统优先级，它的 no 命令用于恢复默认值。

命令

lacp system-priority *value*

no lacp system-priority

参数

value —— 系统优先级，取值范围 0-65535。默认值为 32768。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 1 的系统优先级设置为 1024：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# lacp system-priority 1024

10.5 lacp port-priority

该命令用于配置 LACP 端口优先级，它的 no 命令用于恢复默认值。

命令

lacp port-priority *value*

no lacp port-priority

参数

value —— 端口优先级，取值范围 0-65535。默认值为 32768。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 1 的端口优先级设置为 1024：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# lacp port-priority 1024

10.6 show lacp

该命令用于显示 LACP 全局状态。

命令

show lacp

模式

所有命令模式

示例

显示 LACP 全局状态：

TP-LINK(config)# show lacp

10.7 show lacp interface

该命令用于显示 LACP 端口配置信息。

命令

show lacp interface [**ethernet** *port-num*]

参数

port-num —— 以太网端口号，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示所有端口的配置信息：

```
TP-LINK(config)# show lacp interface
```

第11章 用户管理配置命令

用户配置用来管理通过 Web、CLI 或 SSH 方式登录交换机的用户信息，以达到保护交换机配置的目的。

11.1 user add

该命令用于添加一个新用户账户。

命令

user add *user-name* **password** *password* **confirm-password** *confirm-password* {guest | admin} {disable | enable}

参数

user-name —— 用户名，1-16 个字符，只能由数字、英文字母和下划线组成。

password —— 用户密码，1-16 个字符，只能由数字、英文字母和下划线组成。

confirm-password —— 确认密码，必须跟 password 一致。

guest | admin —— 用户类型，guest：受限用户，admin：管理员。

disable | enable —— 禁用/启用该用户账户。

模式

全局配置模式

示例

添加并启用一个用户名为 tplink，密码为 password 的管理员账户：

TP-LINK(config)#user add tplink **password** password **confirm-password** password admin enable

11.2 user remove

该命令用于删除一个用户账户，该用户必须已存在，并且当前登录用户不能删除本身。

命令

user remove *user-name*

参数

user-name —— 已存在的用户名。

模式

全局配置模式

示例

删除用户名为 tplink 的账户：

TP-LINK(config)# user remove tplink

11.3 user modify status

该命令用于修改用户账户状态。该用户必须已存在，并且当前登录用户不能修改自己的状态。

命令

user modify status *user-name* {disable | enable}

参数

user-name —— 已存在的用户名。

disable | enable —— 禁用/启用该用户账户。

模式

全局配置模式

示例

修改 tplink 账户的状态为启用：

TP-LINK(config)# user modify status tplink enable

11.4 user modify type

该命令用于修改用户账户类型。该用户必须已存在，并且当前登录用户不能修改自己的类型。

命令

user modify type *user-name* {guest | admin}

参数

user-name —— 已存在的用户名。

guest | admin —— 选择用户类型，guest：受限用户，admin：管理员。

模式

全局配置模式

示例

将 tplink 账户设置为管理员：

TP-LINK(config)# user modify type tplink admin

11.5 user modify password

该命令用于修改用户密码。该用户必须已存在。

命令

user modify password *user-name old-password new-password confirm-password*

参数

user-name —— 已存在的用户名。

old-password —— 旧密码。

new-password —— 新密码，1-16 个字符，只能由数字、英文字母和下划线组成。

confirm-password —— 确认密码，必须和新密码一致。

模式

全局配置模式

示例

将 tplink 账户的密码修改为 newpwd：

TP-LINK(config)# user modify password tplink password newpwd newpwd

11.6 user access-control disable

该命令用于取消用户身份限制。

命令

user access-control disable

模式

全局配置模式

示例

禁用用户身份限制：

TP-LINK(config)# user access-control disable

11.7 user access-control ip-based

该命令用于启用基于 IP 地址的身份限制，只有处于所设 IP 网段的设备和当前主机才可以访问本交换机。

命令

user access-control ip-based *ip-addr ip-mask*

参数

ip-addr —— 源 IP 地址。

ip-mask —— IP 掩码。

模式

全局配置模式

示例

启用 IP 地址为 192.168.0.148 的身份限制：

```
TP-LINK(config)# user access-control ip-based 192.168.0.148 255.255.255.0
```

11.8 user access-control mac-based

该命令用于启用基于 MAC 地址的身份限制，只允许所设的 MAC 地址和当前主机的 MAC 地址可以通过 Web 访问交换机。

命令

user access-control mac-based *mac-addr*

参数

mac-addr —— 源 MAC 地址。

模式

全局配置模式

示例

启用 MAC 地址为 00:00:13:0A:00:01 的身份限制：

```
TP-LINK(config)# user access-control mac-based 00:00:13:0A:00:01
```

11.9 user access-control port-based

该命令用于启用基于端口的身份限制，只允许连接在所设的端口上和当前登录用户所连接的端口上的主机可以通过 WEB 访问交换机。

命令

user access-control port-based *port-list*

参数

port-list —— 以太网端口列表，最多可指定 5 个端口。

模式

全局配置模式

示例

启用 2、4、5、6、10 五个端口的身份限制：

```
TP-LINK(config)# user access-control port-based 2,4-6,10
```

11.10 user max-number

该命令用于配置登录人数限制，它的 no 命令用于取消登录人数限制。

命令

user max-number *admin-num* *guest-num*

no user max-number

参数

admin-num —— 管理员账户最大允许登录数，取值范围 1-16。管理员用户和受限用户总数不能超过 16。

guest-num —— 受限用户账户最大允许登录数，取值范围 0-15。管理员用户和受限用户总数不能超过 16。

模式

全局配置模式

示例

设置管理员账户以及受限用户的最大允许登录数分别为 5 和 3：

```
TP-LINK(config)# user max-num 5 3
```

11.11 user idle-timeout

该命令用于连接超时配置，它的 no 命令用于恢复默认的超时时间。

命令

user idle-timeout *minutes*

no user idle-timeout

参数

minutes —— 超时时间，取值范围 5-30（分钟）。默认值为 10。

模式

全局配置模式

示例

将连接超时设置为 15 分钟：

```
TP-LINK(config)# user idle-timeout 15
```

11.12 show user account-list

该命令用于显示当前用户账户列表。

命令

show user account-list

模式

所有命令模式

示例

显示当前用户账户列表：

```
TP-LINK(config)# show user account-list
```

11.13 show user configuration

该命令用于显示用户安全配置，包括身份限制，登录数限制，超时配置等。

命令

show user configuration

模式

所有命令模式

示例

显示用户安全配置：

```
TP-LINK(config)# show user configuration
```

第12章 绑定列表配置命令

四元绑定功能可以将局域网中计算机的 IP 地址、MAC 地址、VLAN 和端口进行绑定，ARP 防护功能以及 IP 源防护功能将使用四元绑定条目对数据包进行过滤。

12.1 binding-table user-bind

该命令用于手动添加 IP-MAC-VID-PORT 四元绑定条目。如果您已经掌握了局域网中计算机用户的相关信息，包括 IP 地址、MAC 地址、VLAN 以及连接端口等，您可以手动对其进行四元绑定。

命令

binding-table user-bind *hostname* *ip-addr* *mac-addr* **vlan** *vid* **port** *port-num* {none | arp-detection | ip-source-guard | both}

参数

hostname —— 需要绑定的主机名，1-20 个字符。

ip-addr —— 源 IP 地址。

mac-addr —— 源 MAC 地址。

vid —— 需要绑定的 VLAN，取值范围 1-4094。

port-num —— 需要绑定的交换机端口号。

{none | arp-detection | ip-source-guard | both}—— 该条目执行的 ACL 动作，arp-detection 表示 ARP 防护；ip-source-guard 表示 IP 源过滤；none 表示两者都不应用；both 表示同时应用于两者。

模式

全局配置模式

示例

手动添加一条四元绑定条目，主机名为 host1，IP 地址为 192.168.0.1，MAC 地址为 00:00:00:00:00:01，VID 为 2，端口号为 5，并将该条目同时应用于 ARP 防护和 IP 源过滤：

TP-LINK(config)# binding-table user-bind host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **port** 5 both

12.2 binding-table remove

该命令用于从绑定表中删除 IP-MAC –VID-PORT 四元绑定条目。

命令

binding-table remove index *idx*

参数

idx —— 指定要删除的条目序号。可使用命令 **show binding-table** 获取各条目对应的序号。注意，这里的序号是指该条目在绑定表中的序号，故显示时不一定是按习惯上的从小到大递增的顺序，而是显示该条目在绑定表中的实际序号。

模式

全局配置模式

示例

删除绑定表中序号为 5 的 IP-MAC –VID-PORT 条目：

TP-LINK(config)# binding-table remove index 5

12.3 dhcp-snooping

该命令用于全局开启 DHCP 侦听功能，它的 no 命令用于禁用 DHCP Snooping。通过 DHCP 侦听功能，交换机可以侦听用户动态申请 IP 地址的过程，并记录局域网中计算机的 IP 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。

命令

dhcp-snooping

no dhcp-snooping

模式

全局配置模式

示例

全局开启 DHCP Snooping：

TP-LINK(config)# dhcp-snooping

12.4 dhcp-snooping global

该命令用于 DHCP Snooping 全局配置，它的 no 命令用于恢复默认配置。

命令

dhcp-snooping global [global-rate{*global-rate*}] [dec-threshold{*dec-threshold*}] [dec-rate{*dec-rate*}]

no dhcp-snooping global

参数

global-rate —— 全局流量控制，配置交换机每秒允许转发的 DHCP 消息的数目，超出

的部分将被丢弃，可选项为 0、10、20、30、40、50，单位 pps（packet/second）。默认值为 0，表示禁用。

dec-threshold —— Decline 保护阀值，配置触发特定端口 Decline 保护所需的 Decline 报文最小流量，可选项为 0、5、10、15、20、25、30，单位 pps（packet/ second）。默认值为 0，表示禁用。

dec- rate —— Decline 保护流量限制，如果端口 Decline 消息流量超出阈值，则将相应端口的端口流量限制设置为该值，可选项为 5、10、15、20、25、30，单位 pps（packet/second）。默认值为 5。

模式

全局配置模式

示例

配置 DHCP Snooping 全局流量控制为 30 pps，Decline 保护阀值为 20 pps，Decline 保护流量阀值为 20 pps：

TP-LINK(config)# dhcp-snooping global global-rate 80 dec-threshold 20 dec-rate 20

12.5 dhcp-snooping information enable

该命令用于开启 DHCP Snooping 的 Option 82 功能，它的 no 命令用于关闭 Option 82 功能。

命令

dhcp-snooping information enable

no dhcp-snooping information enable

模式

全局配置模式

示例

开启 DHCP Snooping 的 Option 82 功能：

TP-LINK(config)# dhcp-snooping information enable

12.6 dhcp-snooping information strategy

该命令用于选择对接收到的包含 Option 82 选项请求报文的配置处理策略，它的 no 命令用于恢复默认选项。

命令

dhcp-snooping information strategy {keep | replace | drop}

no dhcp-snooping information strategy

参数

keep —— 保持该报文中的 Option 82 选项不变并进行转发。默认选项。

replace ——按照配置的填充内容填充 Option 82 选项，并替换报文中原有的 Option 82 选项进行转发。

drop —— 丢弃该报文。

模式

全局配置模式

示例

将接收到的请求报文的 Option 82 选项替换为用户自定义的选项内容，并进行转发：

TP-LINK(config)# dhcp-snooping information strategy replace

12.7 dhcp-snooping information user-defined

该命令用于允许用户自定义 Option 82 选项内容（包括 Remote ID 和 Circuit ID），它的 no 命令用于关闭此功能。

命令

dhcp-snooping information user-defined

no dhcp-snooping information user-defined

模式

全局配置模式

示例

允许用户自定义 Option 82 选项内容：

TP-LINK(config)# dhcp-snooping information user-defined

12.8 dhcp-snooping information remote-id

该命令用于配置 Option 82 的 Remote ID 子选项内容。

命令

dhcp-snooping information remote-id *string*

参数

string —— 用户自定义配置的 Remote ID 子选项内容。长度为 1-32 个字符。

模式

全局配置模式

示例

配置 Option 82 的 Remote ID 子选项为 tplink：

TP-LINK(config)# dhcp-snooping information remote-id tplink

12.9 dhcp-snooping information circuit-id

该命令用于配置 Option 82 的 Circuit ID 子选项内容。

命令

dhcp-snooping information circuit-id *string*

参数

string —— 用户自定义配置的 Circuit ID 子选项内容。长度为 1-32 个字符。

模式

全局配置模式

示例

配置 Option 82 的 Circuit ID 子选项为 tplink:

TP-LINK(config)# dhcp-snooping information circuit-id tplink

12.10 dhcp-snooping trusted

该命令用于配置端口为授信端口，只有授信端口才能接收来自 DHCP 服务器端的消息，它的 no 命令用于取消授信端口配置。

命令

dhcp-snooping trusted

no dhcp-snooping trusted

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用交换机端口 2 为授信端口：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# dhcp-snooping trusted

12.11 dhcp-snooping mac-verify

该命令用于启用端口的 MAC 验证功能，它的 no 命令用于禁用 MAC 验证。DHCP 消息中有两个字

段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

命令

dhcp-snooping mac-verify

no dhcp-snooping mac-verify

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 2 的 MAC 验证功能：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# dhcp-snooping mac-verify

12.12 dhcp-snooping rate-limit

该命令用于配置端口的流量控制，超出流量部分的 DHCP 数据包将被丢弃，它的 no 命令用于恢复默认配置。

命令

dhcp-snooping rate-limit *value*

no dhcp-snooping rate-limit

参数

value —— 端口流量控制，可选项为 0、5、10、15、20、25、30，单位 pps（packet/second）。默认值为 0，表示禁用。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 2 的流量控制设为 20pps：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# dhcp-snooping rate-limit 20

12.13 dhcp-snooping decline

该命令用于启用端口的 decline 侦听功能，它的 no 命令用于禁用 decline 侦听。

命令

dhcp-snooping decline

no dhcp-snooping decline

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 2 的 decline 侦听功能：

```
TP-LINK(config)# interface ethernet  2
TP-LINK(config-if)# dhcp-snooping decline
```

12.14 show binding-table

该命令用于显示 IP-MAC-VID-PORT 四元绑定表。

命令

show binding-table

模式

所有命令模式

示例

显示 IP-MAC-VID-PORT 四元绑定表：

```
TP-LINK(config)# show binding-table
```

12.15 show dhcp-snooping global

该命令用于显示 DHCP Snooping 全局配置信息。

命令

show dhcp-snooping global

模式

所有命令模式

示例

显示 DHCP Snooping 全局配置信息：

```
TP-LINK(config)# show dhcp-snooping global
```

12.16 show dhcp-snooping information

该命令用于显示 DHCP Snooping 的 Option 82 选项配置。

命令

show dhcp snooping information

模式

所有命令模式

示例

显示 DHCP Snooping 的 Option 82 选项配置：

TP-LINK(config)# show dhcp-snooping information

12.17 show dhcp-snooping interface

该命令用于显示 DHCP Snooping 端口配置信息。

命令

show dhcp snooping interface [**ethernet** *port-num*]

参数

port-num —— 交换机端口号，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示所有端口的 DHCP Snooping 配置信息：

TP-LINK(config)# show dhcp-snooping interface

第13章 ARP防护配置命令

防 ARP 欺骗功能可以针对局域网中常见的网关欺骗和中间人攻击等 ARP 欺骗进行防护，有效抑制局域网中的 ARP 欺骗。

13.1 arp detection (global)

该命令用于全局开启 ARP 防护，它的 no 命令用于禁用 ARP 防护功能。

命令

arp detection

no arp detection

模式

全局配置模式

示例

全局开启 ARP 防护：

```
TP-LINK(config)# arp detection
```

13.2 arp detection trust-port

该命令用于配置 ARP 防护的信任端口，它的 no 命令用于清空信任端口列表。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

命令

arp detection trust-port *port-list*

no arp detection trust-port

参数

port-list —— 指定信任端口列表。

模式

全局配置模式

示例

配置端口 2-5,11-15 为 ARP 防护的信任端口：

```
TP-LINK(config)# arp detection trust-port  2-5,11-15
```

13.3 arp detection (interface)

该命令用于开启端口的 ARP 超速防护，它的 no 命令用于禁用 ARP 超速防护。

命令

arp detection

no arp detection

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 2-6 的 ARP 超速防护：

TP-LINK(config)# interface range ethernet 2-6

TP-LINK(config-if)# arp detection

13.4 arp detection limit-rate

该命令用于配置端口的 ARP 超速速率，它的 no 命令用于恢复默认超速速率。

命令

arp detection limit-rate *value*

no arp detection limit-rate

参数

value —— 超速速率值，取值范围 10-100，单位 pps（packet/second）。默认值为 15。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 5 的 ARP 超速速率设置为 50pps：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# arp detection limit-rate 50

13.5 arp detection recover

该命令用于将处于 ARP 过滤状态的端口恢复为 ARP 转发状态。

命令

arp detection recover

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

将端口 5 恢复为 ARP 转发状态：

```
TP-LINK(config)# interface ethernet   5
TP-LINK(config-if)# arp detection recover
```

13.6 show arp detection global

该命令用于显示 ARP 防护全局配置，包括启用状态和信任端口列表。

命令

show arp detection global

模式

所有命令模式

示例

显示 ARP 防护全局配置：

```
TP-LINK(config)# show arp detection global
```

13.7 show arp detection interface

该命令用于显示 ARP 防护端口配置信息。

命令

show arp detection interface [**ethernet** *port-num*]

参数

port-num —— 交换机端口号，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示所有端口的 ARP 防护配置信息：

```
TP-LINK(config)# show arp detection interface
```

13.8 show arp detection statistic

该命令用于显示 ARP 非法报文统计。

命令

show arp detection statistic

模式

所有命令模式

示例

显示 ARP 非法报文统计：

```
TP-LINK(config)# show arp detection statistic
```

13.9 arp detection reset-statistic

该命令用于对 ARP 非法报文统计进行清零。

命令

arp detection reset-statistic

模式

全局配置模式

示例

对 ARP 非法报文统计进行清零：

```
TP-LINK(config)# arp detection reset-statistic
```

第14章 IP源防护配置命令

IP 源防护功能是交换机根据四元绑定条目对接收的 IP 包进行过滤，只处理数据包相关字段与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

14.1 ip source guard

该命令用于启用端口的 IP 源防护功能，它的 no 命令用于禁用端口的 IP 源防护。

命令

ip source guard {diable | sip | sip+mac}

no ip source guard

参数

diable | sip | sip+mac—— 防护类型，disable 表示禁用；sip 表示源 IP 地址；sip_mac 表示源 IP 地址和 MAC 地址。默认选项为 disable。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用 5-10 端口的 IP 源防护功能，设定为只处理源 IP 地址、源 MAC 地址和端口均符合四元绑定信息的数据包：

TP-LINK(config)# interface range ethernet 5-10

TP-LINK(config-if)# ip source guard sip+mac

14.2 show ip source guard

该命令用于显示 IP 源防护配置信息。

命令

show ip source guard

模式

所有命令模式

示例

显示 IP 源防护配置信息：

TP-LINK(config)# show ip source guard

第15章 DoS防护命令

DoS 攻击是指网络中攻击者或者恶意程序向目标主机发送大量的服务请求，恶意消耗网络资源。启用 DoS 防护功能后，交换机对收到的特殊数据包的特定字段进行解析，并针对这些信息定义防护措施，从而保护局域网的正常运行。

15.1 dos-prevent

该命令用于全局启用 DoS 防护功能，它的 no 命令用于禁用 DoS 防护功能。

命令

dos-prevent

no dos-prevent

模式

全局配置模式

示例

全局启用 DoS 防护功能：

```
TP-LINK(config)# dos-prevent
```

15.2 dos-prevent global

该命令用于配置 Ping Flooding 限速和 SYN Flooding 限速，它的 no 命令用于恢复默认配置。

命令

dos-prevent global *ping-rate syn-rate*

no dos-prevent global

参数

ping-rate —— Ping Flooding 限速，可选项为 128k、256k、512k、1m、2m、4m，单位 bps。默认值为 128k。

syn-rate —— SYN Flooding 限速，可选项为 128k、256k、512k、1m、2m、4m，单位 bps。默认值为 128k。

模式

全局配置模式

示例

配置 Ping Flooding 限速和 SYN Flooding 限速分别为 256k 和 1m：

TP-LINK(config)# dos-prevent global 256k 1m

15.3 dos-prevent type

该命令用于启用 DoS 攻击防护类型，它的 no 命令用于禁用相应的防护类型。

命令

dos-prevent type [land] [scan-synfin] [xma-scan] [null-scan] [port-less -1024] [smurf] [blat] [ping-flood] [syn-flood] [win-nuke]

no dos-prevent type [land] [scan-synfin] [xma-scan] [null-scan] [port-less -1024] [smurf] [blat] [ping-flood] [syn-flood]

参数

land —— Land 攻击。

scan-synfin —— Scan SYNFIN 攻击。

xma-scan —— Xma Scan 攻击。

null-scan —— NULL Scan 攻击。

port-less-than-1024 —— 源端口小于 1024 的 SYN 报文。

smurf —— Smurf 攻击。

blat —— Blat 攻击。

ping-flood —— Ping flooding 攻击。

syn-flood —— SYN/SYN-ACK flooding 攻击。

win-nuke —— winNuke Attack 攻击。

模式

全局配置模式

示例

启用防 Land 攻击，Xma Scan 攻击，Smurf 攻击，Ping flooding 攻击等四种 DoS 攻击的防护功能：

TP-LINK(config)# dos-prevent land xma-scan smurf ping-flood

15.4 dos-prevent detect

该命令用于进行 DoS 攻击检测。通过攻击检测功能，您可以检测各端口收到的 DoS 攻击详细情况，帮助您迅速定位局域网中的攻击者位置。

命令

dos-prevent detect *detect-time*

参数

detect-time ——配置除了泛洪攻击类型外每种攻击类型的检测时间长度，取值范围为 1-5 秒。

模式

全局配置模式

示例

进行 DoS 攻击检测，每种攻击类型的检测时间为 5 秒：

```
TP-LINK(config)# dos-prevent   detect   5
```

15.5 dos-prevent reset-statistic

该命令用于对 DoS 攻击统计信息进行清零。

命令

dos-prevent reset-statistic

模式

全局配置模式

示例

对 DoS 攻击统计信息进行清零：

```
TP-LINK(config)# dos-prevent   reset-statistic
```

15.6 show dos-prevent

该命令用于显示 DoS 攻击防护全局配置信息，包括启用状态、攻击防护类型、攻击次数统计等。

命令

show dos-prevent

模式

所有命令模式

示例

显示 DoS 攻击防护全局配置信息：

```
TP-LINK(config)# show dos-prevent
```

第16章 IEEE 802.1X配置命令

IEEE 802.1X 能为局域网计算机提供认证功能，并根据认证结果对受控端口的授权状态进行控制，主要用于解决以太网内认证和安全方面的问题。

16.1 dot1x

该命令用于全局开启 IEEE 802.1X 功能，它的 no 命令用于禁用 IEEE 802.1X 功能。

命令

dot1x

no dot1x

模式

全局配置模式

示例

开启 IEEE 802.1X 功能：

```
TP-LINK(config)# dot1x
```

16.2 dot1x authentication-method

该命令用于配置 IEEE 802.1X 的认证方法，它的 no 命令用于恢复默认配置。

命令

dot1x authentication-method { pap | eap-md5 }

no dot1x authentication-method

参数

pap | eap-md5 —— 认证方法。选择 pap 时，用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。选择 eap-md5 时，交换机与认证服务器之间运行 EAP 协议，EAP 帧中继封装认证数据，将该协议承载在其它高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器。默认选项为 eap-md5。

模式

全局配置模式

示例

设置 IEEE 802.1X 认证方法为 pap：

```
TP-LINK(config)# dot1x authentication-method pap
```

16.3 dot1x guest-vlan

该命令用于全局开启 Guest VLAN 功能，它的 no 命令用于全局禁用 Guest VLAN 功能。

命令

dot1x guest-vlan *vid*

no dot1x guest-vlan

参数

vid —— 启用 Guest VLAN 的 VLAN ID，取值范围 2~4094。Guest VLAN 中的用户可以访问指定的网络资源。

模式

全局配置模式

示例

启用 VLAN 5 为 Guest VLAN：

```
TP-LINK(config)# dot1x guest-vlan 5
```

16.4 dot1x quiet-period

该命令用于开启 IEEE 802.1X 特性的静默功能，它的 no 命令用于关闭该功能。

命令

dot1x quiet-period

no dot1x quiet-period

模式

全局配置模式

示例

开启 IEEE 802.1X 静默功能：

```
TP-LINK(config)# dot1x quiet-period
```

16.5 dot1x timer

该命令用于配置静默时长、客户端响应超时时长，它的 no 命令用于恢复默认配置。

命令

dot1x timer quiet-period *period* **supp-timeout** *timeout*

no dot1x timer

参数

period —— 静默时长。用户认证失败后，在静默时间内不再处理同一用户的 IEEE 802.1X 认证请求。取值范围 1~999（秒），默认值为 10。

timeout —— 客户端响应超时时长，即交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。取值范围 1~9（秒），默认值为 3。

模式

全局配置模式

示例

设置静默时长为 12 秒，客户端响应超时时长为 6 秒：

```
TP-LINK(config)# dot1x timer quiet-period 12 supp-timeout 6
```

16.6 dot1x retry

该命令用于配置客户端请求报文重复发送次数，它的 no 命令用于恢复默认设置。

命令

dot1x retry *retry-time*

no dot1x retry

参数

retry-time —— 认证报文的最大重复发送次数，取值范围 1~9（次），默认值为 3。

模式

全局配置模式

示例

设置最大重复发送次数为 5：

```
TP-LINK(config)# dot1x retry 5
```

16.7 dot1x

该命令用于开启端口的 IEEE 802.1X 特性，它的 no 命令用于禁用端口的 IEEE 802.1X 特性。

命令

dot1x

no dot1x

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 1 的 IEEE 802.1X 特性：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# dot1x

16.8 dot1x guest-vlan

该命令用于开启端口的Guest VLAN功能，它的no命令用于禁用端口的Guest VLAN功能。在开启端口的Guest VLAN功能前，请确保相应端口的接入控制类型为port-based，详见 dot1x port-method。

命令

dot1x guest-vlan

no dot1x guest-vlan

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 2 的 Guest VLAN 功能：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# dot1x guest-vlan

16.9 dot1x port-control

该命令用于配置 IEEE 802.1X 在指定端口的接入控制模式，它的 no 命令用于恢复默认配置。

命令

dot1x port-control { auto | authorized-force | unauthorized-force }

no dot1x port-control

参数

auto | authorized-force | unauthorized-force —— 控制模式，有 auto（自动）、authorized-force（强制已认证）、unauthorized-force（强制不认证）三个选项。选择 auto 时，端口需要进行认证；选择 authorized-force 时，端口不需认证即可访问网络；选择 unauthorized-force 时，端口永远无法通过认证。默认选项为 auto。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置端口 1 的接入控制模式为强制已认证：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# dot1x port-control authorized-force

16.10 dot1x port-method

该命令用于配置 IEEE 802.1X 在指定端口的接入控制类型，它的 no 命令用于恢复默认配置。

命令

dot1x port-method { mac-based | port-based }

no dot1x port-method

参数

mac-based | port-based —— 控制类型，有 mac-based（基于 MAC）和 port-based（基于 Port）两个选项。选择 mac-based 时，该端口连接的所有计算机都需认证；选择 port-based 时，该端口连接的某个用户通过认证后，其他用户均无须认证即可访问网络。默认选项为 mac-based。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置端口 5 的接入控制类型为基于 Port 认证：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# dot1x port-method port-based

16.11 radius authentication primary-ip

该命令用于配置主认证服务器的 IP 地址。认证服务器是为交换机提供认证服务的实体。认证服务器可以存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户的认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

命令

radius authentication primary-ip *ip-addr*

参数

ip-addr —— 主认证服务器的 IP 地址。

模式

全局配置模式

示例

设置主认证服务器的 IP 地址为 10.20.1.100：

TP-LINK(config)# radius authentication primary-ip 10.20.1.100

16.12 radius authentication secondary-ip

该命令用于配置备份认证服务器的 IP 地址，它的 no 命令用于恢复默认配置。

命令

radius authentication secondary-ip *ip-addr*

no radius authentication secondary-ip

参数

ip-addr —— 备份认证服务器的 IP 地址，默认情况下为 0.0.0.0。

模式

全局配置模式

示例

设置备份认证服务器的 IP 地址为 10.20.1.101：

TP-LINK(config)# radius authentication secondary-ip 10.20.1.101

16.13 radius authentication port

该命令用于配置认证服务器的认证端口，它的 no 命令用于恢复默认值。

命令

radius authentication port *port-num*

no radius authentication port

参数

port-num —— 认证服务器提供认证服务的协议端口。取值范围 1~65535，默认值为 1812。

模式

全局配置模式

示例

设置认证服务器的认证端口为 1815：

TP-LINK(config)# radius authentication port 1815

16.14 radius authentication key

该命令用于配置认证服务器的共享密钥，它的 no 命令用于清空认证密钥。

命令

radius authentication key *key-string*

no radius authentication key

参数

key-string —— 授权共享密钥，即交换机与服务器共享的密钥。可输入 1~15 个字符。

模式

全局配置模式

示例

设置认证服务器的共享密钥为 tplink：

TP-LINK(config)# radius authentication key tplink

16.15 radius accounting enable

该命令用于启用计费服务器的计费功能，它的 no 命令用于禁用计费功能。

命令

radius accounting enable

no radius accounting enable

模式

全局配置模式

示例

启用计费功能：

TP-LINK(config)# radius accounting enable

16.16 radius accounting primary-ip

该命令用于配置主计费服务器的 IP 地址。

命令

radius accounting primary-ip *ip-addr*

参数

ip-addr —— 主计费服务器的 IP 地址。

模式

全局配置模式

示例

设置主计费服务器的 IP 地址为 10.20.1.100：

TP-LINK(config)# radius accounting primary-ip 10.20.1.100

16.17 radius accounting secondary-ip

该命令用于配置备份计费服务器的 IP 地址，它的 no 命令用于恢复默认配置。

命令

radius accounting secondary-ip *ip-addr*

no radius accounting secondary-ip

参数

ip-addr —— 备份计费服务器的 IP 地址，默认情况下为 0.0.0.0。

模式

全局配置模式

示例

设置备份计费服务器的 IP 地址为 10.20.1.101：

TP-LINK(config)# radius accounting secondary-ip 10.20.1.101

16.18 radius accounting port

该命令用于配置计费服务器的计费端口，它的 no 命令用于恢复默认值。

命令

radius accounting port *port-num*

no radius accounting port

参数

port-num —— 计费服务器提供计费服务的协议端口。取值范围 1~65535，默认值为 1813。

模式

全局配置模式

示例

设置计费服务器的计费端口为 1816：

TP-LINK(config)# radius accounting port 1816

16.19 radius accounting key

该命令用于配置计费服务器的共享密钥，它的 no 命令用于清空计费密钥。

命令

radius accounting key *key-string*

no radius accounting key

参数

key-string —— 授权共享密钥，即交换机与服务器共享的密钥。可输入 1~15 个字符。

模式

全局配置模式

示例

设置计费服务器的共享密钥为 tplink：

TP-LINK(config)# radius accounting key tplink

16.20 radius response-timeout

该命令用于配置 RADIUS 认证和计费服务器的响应超时时间，它的 no 命令用于恢复默认值。

命令

radius response-timeout *time*

no radius response-timeout

参数

time —— 服务器响应超时时间，即交换机等待服务器响应的最大等待时间。若交换机在设定时间内没有收到服务器的回复，则重发报文。取值范围 1~9（秒），默认值为 3。

模式

全局配置模式

示例

设置 RADIUS 认证和计费服务器的响应超时时间为 5 秒：

TP-LINK(config)# radius response-timeout 5

16.21 show dot1x global

该命令用于显示 801.X 全局配置信息。

命令

show dot1x global

模式

所有命令模式

示例

显示 801.X 全局配置信息：

```
TP-LINK(config)# show dot1x global
```

16.22 show dot1x interface

该命令用于显示 801.X 端口配置信息。

命令

show dot1x interface [**ethernet** *port-num*]

参数

port-num —— 以太网端口号，取值范围 1~28。缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示 801.X 端口配置信息：

```
TP-LINK(config)# show dot1x interface
```

16.23 show radius authentication

该命令用于显示 RADIUS 认证服务器的配置信息。

命令

show radius authentication

模式

所有命令模式

示例

显示 RADIUS 认证服务器配置信息：

```
TP-LINK(config)# show radius authentication
```

16.24 show radius accounting

该命令用于显示 RADIUS 计费服务器的配置信息。

命令

show radius accounting

模式

所有命令模式

示例

显示 RADIUS 计费服务器配置信息：

```
TP-LINK(config)# show radius accounting
```

第17章 系统日志配置命令

系统日志信息对交换机的配置和运行进行分类记载，为监控设备的运行状态和诊断设备故障提供支持。

17.1 logging local buffer

该命令用于配置系统日志缓冲区的信息输入等级和状态，它的no命令用于恢复默认设置。保存在本设备上的系统日志信息为本地日志，本地日志有两个输出方向（即可以保存到两个不同的地方）：日志缓冲区和日志文件。日志缓冲区是用于保存系统日志的一块内存区域，缓冲区中的信息可通过**show logging buffer**命令查看，在断电重启后这些信息将会丢失。本命令用来配置日志缓冲区的相关参数。

命令

logging local buffer {*level*} [disable | enable]

no logging local buffer

参数

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志缓冲区。默认值为 7，表示所有日志信息都保存到日志缓冲区。

disable | enable —— 禁用或启用日志缓冲区，默认为启用（enable）。

模式

全局配置模式

示例

启用日志缓冲区并设置严重级别为 6：

TP-LINK(config)# logging local buffer 6 enable

17.2 logging local flash

该命令用于配置系统日志文件的信息输入等级和状态，它的no命令用于恢复默认设置。日志文件是Flash里的一块存储区域。日志文件的信息可通过 **show logging flash**命令查看，在断电重启后这些信息不会丢失。

命令

logging local flash {*level*} [disable | enable]

no logging local flash

参数

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志文件中。默认值为 4，表示允许级别为 0~4 的日志信息保存到日志文件中。

disable | enable —— 禁用或启用日志文件，默认为启用（enable）。

模式

全局配置模式

示例

启用日志文件并设置严重级别为 7：

TP-LINK(config)# logging local flash 7

17.3 logging clear

该命令用于清空当前日志缓冲区或日志文件中的信息。

命令

logging clear [buffer | flash]

参数

buffer | flash —— 要清空的输出方向，有 buffer（日志缓冲区）和 flash（日志文件）两个选项，缺省时表示两者的信息都被清空。

模式

全局配置模式

示例

清空当前日志缓冲区中的系统日志信息：

TP-LINK(config)# logging clear buffer

17.4 logging loghost

该命令用于配置日志服务器，它的 no 命令用于清空指定日志服务器的配置信息。日志服务器用于接收其他设备发送的系统日志消息，通过日志服务器可以对其他设备的配置情况和运行状态进行远程监控。

命令

logging loghost index {*idx*} {*host-ip*} {*level*} { disable | enable }

no logging loghost index {*idx*}

参数

idx —— 日志服务器的序号，取值范围 1~4。

host-ip —— 日志服务器的 IP 地址。

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息发送到该服务器。默认值为 6，表示允许级别为 0~6 的日志信息发送到该服务器。

disable | enable —— 禁用或启用指定的日志服务器，默认为禁用（disable）。

模式

全局配置模式

示例

启用日志服务器 2，并设置该服务器的 IP 地址为 192.168.0.148，严重级别为 5：

TP-LINK(config)# logging loghost index 2 192.168.0.148 5 enable

17.5 show logging local-config

该命令用于显示本地日志（包括日志缓冲区和日志文件）的配置信息。

命令

show logging local-config

模式

所有命令模式

示例

显示本地日志配置信息：

TP-LINK(config)# show logging local-config

17.6 show logging loghost

该命令用于显示日志服务器的配置信息。

命令

show logging loghost [*index*]

参数

index —— 要显示配置信息的日志服务器序号，缺省时显示所有日志服务器的配置信息。

模式

所有命令模式

示例

显示日志服务器 2 的配置信息：

TP-LINK(config)# show logging loghost 2

17.7 show logging buffer

该命令用于显示日志缓冲区中的日志信息，可根据严重级别进行过滤显示。

命令

show logging buffer [*level*]

参数

level —— 严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志缓冲区中的所有日志信息。

模式

所有命令模式

示例

显示日志缓冲区中的所有日志信息：

TP-LINK(config)# show logging buffer

17.8 show logging flash

该命令用于显示日志文件中的日志信息，可根据严重级别进行过滤显示。

命令

show logging flash [*level*]

参数

level —— 严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志文件中的所有日志信息。

模式

所有命令模式

示例

显示日志文件中级别为 0~3 的日志信息：

TP-LINK(config)# show logging flash 3

第18章 SSH配置命令

SSH（Security Shell）采用加密和认证功能，可以为远程登录管理提供安全保障，以保证管理信息的安全。

18.1 ssh server enable

该命令用于启用 SSH 服务器功能，它的 no 命令用于禁用 SSH 服务器功能。

命令

ssh server enable

no ssh server enable

模式

全局配置模式

示例

启用 SSH 服务器功能：

TP-LINK(config)# ssh server enable

18.2 ssh version

该命令用于启用 SSH 的协议版本，它的 no 命令用于禁用 SSH 协议版本。

命令

ssh version { v1 | v2 }

no ssh version { v1 | v2 }

参数

v1 | v2 —— 要启用的 SSH 协议版本，分别对应 SSH v1 和 SSH v2。

模式

全局配置模式

示例

启用 SSH v2：

TP-LINK(config)# ssh version v2

18.3 ssh idle-timeout

该命令用于设置 SSH 的静默时长，它的 no 命令用于恢复默认配置。

命令

ssh idle-timeout *value*

no ssh idle-timeout

参数

value —— 静默时长，当此时间内客户端未有动作时，连接会自动断开。单位为秒，取值范围 1~999，默认值为 500。

模式

全局配置模式

示例

配置 SSH 静默时长为 300 秒：

TP-LINK(config)# ssh idle-timeout 300

18.4 ssh max-client

该命令用于配置 SSH 的最大连接数，它的 no 命令用于恢复默认配置。

命令

ssh max-client *number*

no ssh max-client

参数

number —— SSH 最大连接数，取值范围 1~5，默认值为 5。

模式

全局配置模式

示例

配置 SSH 最大连接数为 3：

TP-LINK(config)# ssh max-client 3

18.5 ssh download

该命令用于通过 TFTP 方式导入 SSH 密钥文件。

命令

ssh download { v1 | v2 } *key-file* **ip-address** *ip-addr*

参数

v1 | v2 —— 选择要导入的密钥类型，v1 表示 SSH-1，v2 表示 SSH-2。

key-file —— 选择要导入的密钥文件名称，可输入 1~25 个字符。导入的文件必须是密钥长度为 256~3072 比特的 SSH 公钥。

ip-addr —— TFTP 服务器的 IP 地址。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssh-key 的 SSH-1 密钥文件：

TP-LINK(config)# ssh download v1 ssh-key **ip-address** 192.168.0.148

18.6 show ssh

该命令用于显示 SSH 的全局配置信息。

命令

show ssh

模式

所有命令模式

示例

显示 SSH 全局配置信息：

TP-LINK(config)# show ssh

第19章 SSL配置命令

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 采用非对称加密技术，用密钥对进行信息的加密/解密，密钥对由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名证书）和对应私钥，用户也可以通过证书/密钥导入功能替换默认的密钥对。

19.1 ssl enable

该命令用于全局开启 SSL 功能，它的 no 命令用于禁用 SSL 功能。只有开启 SSL 功能，才能进行 HTTPS 安全连接。

命令

ssl enable

no ssl enable

模式

全局配置模式

示例

全局开启 SSL 功能：

TP-LINK(config)# ssl enable

19.2 ssl download certificate

该命令用于通过 TFTP 方式导入 SSL 证书。

命令

ssl download certificate *ssl-cert* **ip-address** *ip-addr*

参数

ssl-cert —— 选择要导入的 SSL 证书名称，可输入 1~25 个字符。证书必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssl-cert 的 SSL 证书：

TP-LINK(config)# ssl download certificate ssl-cert **ip-address** 192.168.0.148

19.3 ssl download key

该命令用于通过 TFTP 方式导入 SSL 密钥。

命令

ssl download key *ssl-key* **ip-address** *ip-addr*

参数

ssl-key —— 选择要导入的 SSL 密钥文件名称，可输入 1~25 个字符。密钥必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssl-key 的 SSL 密钥：

```
TP-LINK(config)# ssl download key ssl-key ip-address 192.168.0.148
```

19.4 show ssl

该命令用于显示 SSL 的全局配置信息。

命令

show ssl

模式

所有命令模式

示例

显示 SSL 全局配置信息：

```
TP-LINK(config)# show ssl
```

第20章 地址配置命令

地址配置通过端口安全设置和地址表管理来提高网络安全，管理地址信息。

20.1 bridge address port-security

该命令用于设置端口安全参数，它的 no 命令用于恢复默认配置。端口安全通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击和控制端口的网络流量。如果端口启用端口安全功能，将自动学习接入设备的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，保证安全性。

命令

bridge address port-security [**max-number** {*num*}] [**mode** {dynamic | static | permanent}] [**state** {disable | enable}]

no bridge address port-security

参数

num —— 端口最多可以学习的 MAC 地址数目，取值范围 0~64，缺省时为 64。

mode —— 端口地址学习模式，有 dynamic（动态）、static（静态）和 permanent（永久）三个选项。选择 dynamic 时，MAC 地址学习受老化时间的限制，老化时间过后，所学的 MAC 地址将被删除；选择 static 时，MAC 地址学习不受老化时间的限制，只能手动进行删除，但交换机重启后学习到的条目将清空；选择 permanent 时，MAC 地址学习不受老化时间的限制，只能手动进行删除，交换机重启后学习到的条目保持不变。缺省时为 dynamic。

state —— 是否启用端口安全功能，默认为禁用（disable）。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 1 的安全功能，并设置学习模式为静态，最大可学习 MAC 地址数为 30：

```
TP-LINK(config)# interface ethernet 1
TP-LINK(config-if)# bridge address port-security max-number 30 mode static state enable
```

20.2 bridge address static

该命令用于添加静态地址条目，它的 no 命令用于删除对应条目。静态地址由用户手工添加和删除，

不受老化时间的限制。对于网络拓扑相对固定的使用环境来说，使用静态地址绑定可以提高交换机的转发效率，减少网络中的广播流量。

命令

bridge address static {**mac** *mac*} {**vid** *vid*} {**port** *port*}

no bridge address static [*mac*] [*vid*] [*port*]

参数

mac —— 要添加的地址条目的 MAC 地址。

vid —— 地址条目所属的 VLAN ID，取值范围 1~4094。

port —— 地址条目对应的端口，取值范围 1~28。

模式

全局配置模式

示例

添加静态地址条目，该条目将 MAC 地址 00:02:58:4f:6c:23、VLAN1 和端口 1 绑定：

TP-LINK(config)# bridge address static mac 00:02:58:4f:6c:23 **vid** 1 **port** 1

20.3 bridge aging-time

该命令用于配置动态地址老化时间，它的 no 命令用于恢复默认配置。

命令

bridge aging-time *aging-time*

no bridge aging-time

参数

aging-time —— 要设置的地址老化时间，取值范围为 0 或 10~630（秒），为 0 时表示不启用自动老化功能。默认值为 300。

模式

全局配置模式

示例

设置地址老化时间为 500 秒：

TP-LINK(config)# bridge aging-time 500

20.4 bridge address filtering

该命令用于添加过滤地址条目，它的 no 命令用于删除对应条目。通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤。过滤地址不会被老化，只能手动进行配置和删除。

命令

bridge address filtering {*mac*} {*vid*}

no bridge address filtering [*mac*] [*vid*]

参数

mac —— 要添加的地址条目的 MAC 地址。

vid —— 地址条目所属的 VLAN ID，取值范围 1~4094。

模式

全局配置模式

示例

添加过滤地址条目，过滤 VLAN1 的 MAC 地址 00:1e:4b:04:01:5d：

TP-LINK(config)# bridge address filtering 00:1e:4b:04:01:5d 1

20.5 show bridge dynamic-bind

该命令用于显示端口的安全配置，即端口最大可学习 MAC 地址数和学习模式。

命令

show bridge dynamic-bind [*port-num*]

参数

port-num —— 要显示安全配置信息的端口号，取值范围 1~28，缺省时显示所有端口的安全配置信息。

模式

所有命令模式

示例

显示端口 2 的安全配置信息：

TP-LINK(config)# show bridge dynamic-bind 2

20.6 show bridge address

该命令用于显示地址条目信息。

命令

show bridge address { dynamic | static | filter | all }

参数

dynamic | static | filter | all —— 要显示的地址类型。

模式

所有命令模式

示例

显示所有地址条目信息：

TP-LINK(config)# show bridge address all

20.7 show bridge aging-time

该命令用于显示地址老化时间。

命令

show bridge aging-time

模式

所有命令模式

示例

显示地址老化时间：

TP-LINK(config)# show bridge aging-time

第21章 系统配置命令

系统配置用来配置系统信息、IP 地址等参数，并且可以对交换机进行重启、复位、升级系统文件等操作。

21.1 system-descript

该命令用于设置系统名称、系统位置和联系方法，它的 no 命令用于清空相应信息。

命令

system-descript { **sysname** {*sysname*} | **location** {*location*} | **contact-info** {*contact_info*} }

no system-descript {sysname | location | contact_info}

参数

sysname —— 系统名称，1~32 个字符，默认为空。

location —— 系统位置，1~32 个字符，默认为空。

contact_info —— 联系方法，1~32 个字符，默认为空。

模式

全局配置模式

示例

设置联系方法为 www.tp-link.com.cn：

```
TP-LINK(config)# system-descript contact-info www.tp-link.com.cn
```

21.2 ip address

该命令用于设置系统的 IP 地址，子网掩码和默认网关，它的 no 命令用于恢复默认设置。

命令

ip address {*ip-addr*} {*ip-mask*} [*gateway*]

no ip address

参数

ip-addr —— 系统 IP 地址，默认为 192.168.0.1。

ip-mask —— 系统子网掩码，默认为 255.255.255.0。

gateway —— 系统网关，默认为空。

模式

全局配置模式

示例

将系统的 IP 地址设置为 192.168.0.69，子网掩码设置为 255.255.255.0：

TP-LINK(config)# ip address 192.168.0.69 255.255.255.0

21.3 ip dhcp-alloc

该命令用于启用 DHCP Client 功能，通过 DHCP Client 方式获取 IP 地址。它的 no 命令用于禁用 DHCP Client 功能。

命令

ip dhcp-alloc

no ip dhcp-alloc

模式

全局配置模式

示例

开启系统的 DHCP Client 功能：

TP-LINK(config)# ip dhcp-alloc

21.4 ip bootp-alloc

该命令用于通过 BOOTP 协议获取 IP 地址，它的 no 命令用于取消通过 BOOTP 协议获取 IP 地址。

命令

ip bootp-alloc

no ip bootp-alloc

模式

全局配置模式

示例

启用 BOOTP 协议，通过 BOOTP 协议来获取 IP 地址：

TP-LINK(config)# ip bootp-alloc

21.5 reset

该命令用于把交换机软件复位，软件复位后，交换机配置（除 IP 地址不变外）将恢复成出厂默认状态，用户配置数据将丢失。

命令

reset

模式

特权模式

示例

对交换机进行软件复位：

TP-LINK# reset

21.6 reboot

该命令用于重启交换机。在重启期间，请注意不要关闭设备电源，以免损坏设备。

命令

reboot

模式

特权模式

示例

重新启动交换机：

TP-LINK# reboot

21.7 user-config backup

该命令用于通过 TFTP 方式导出配置文件。

命令

user-config backup filename *name* **ip-address** *ip-addr*

参数

name —— 指定导出的配置文件名。

ip-addr —— TFTP 服务器的 IP 地址。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导出配置文件，并将导出的配置文件命名为 config.cfg：

TP-LINK# user-config backup filename config.cfg **ip-address** 192.168.0.148

21.8 user-config load

该命令用于通过 TFTP 方式导入配置文件。

命令

user-config load filename *name* **ip-address** *ip-addr*

参数

name —— 要导入的配置文件名。

ip-addr —— TFTP 服务器的 IP 地址。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 config.cfg 的配置文件：

TP-LINK# user-config load filename config.cfg **ip-address** 192.168.0.148

21.9 user-config save

该命令用于保存当前用户配置。

命令

user-config save

模式

特权模式

示例

保存当前用户的配置：

TP-LINK# user-config save

21.10 firmware upgrade

该命令用于通过 TFTP 方式升级系统文件。

命令

firmware upgrade filename *name* **ip-address** *ip-addr*

参数

name —— 指定系统文件名。

ip-addr —— TFTP 服务器的 IP 地址。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器升级系统文件：

TP-LINK# firmware upgrade filename firmware.bin **ip-address** 192.168.0.148

21.11 ping

该命令用于检测从交换机到某一网络节点之间的链路是否连通。

命令

ping {*ip_addr*} [**-n** {*count*}] [**-l** {*count*}] [**-i** {*count*}]

参数

ip_addr ——要检测的目标节点的 IP 地址。

count (-n) —— 发送报文的次数，取值范围 1~10，默认值为 4。

count (-l) —— 发送报文的长度，取值范围 1~1024（字节），默认值为 64。

count (-i) —— 发送报文的时间间隔，取值范围 100~1000（毫秒），默认值为 1000。

模式

用户模式和特权模式

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，其中测试报文的长度为 512 字节，报文每隔 1000 毫秒发送一次，若发送 8 次后没有收到回复，则判断为连接失败：

TP-LINK# ping 192.168.0.131 **–n** 8 **–l** 512

21.12 tracert

该命令用于检测测试报文从交换机传送到目的设备所经过的网关的连通性。

命令

tracert {*url*} [*maxHops*]

参数

url ——要检测的目的设备的 IP 地址。

maxHops —— 最大路由跳数，取值范围 1~30，默认值为 4。

模式

用户模式和特权模式

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，若经过 20 跳路由后仍未连通，则判断为连接失败：

TP-LINK# tracert 192.168.0.131 20

21.13 loopback

该命令用于检查端口的可用性。

命令

loopback {*port*} { internal | external }

参数

port —— 要检测的端口号，取值范围 1~28。

internal | external —— 检测类型，有 internal（内环检测）和 external（外环检测）两个选项。

模式

用户模式和特权模式

示例

对端口 4 进行内环检测：

TP-LINK#loopback 4 internal

21.14 show system-info

该命令用于显示系统描述、系统名称、系统位置、联系方法、硬件版本、软件版本、系统时间和运行时间等信息。

命令

show system-info

模式

所有命令模式

示例

显示系统信息：

TP-LINK# show system-info

21.15 show ip address

该命令用于显示系统的 MAC 地址、IP 地址、子网掩码、网关及是否开启了 DHCP Client 功能等信息。

命令

show ip address

模式

所有命令模式

示例

显示系统的 IP 地址等信息：

```
TP-LINK# show ip address
```

第22章 以太网配置命令

以太网配置用来配置以太网端口的流量控制、协商模式、风暴抑制、带宽限制等。

22.1 interface ethernet

该命令用于进入接口配置命令模式，对单个以太网端口进行配置。

命令

interface ethernet *interface*

参数

interface —— 要配置的以太网端口。

模式

全局配置模式

示例

进入接口配置模式，对以太网端口 2 进行配置：

```
TP-LINK(config)# interface ethernet 2
```

22.2 interface range ethernet

该命令用于进入接口配置命令模式，对多个以太网端口进行同时配置。

命令

interface range ethernet *port-list*

参数

port-list —— 要配置的以太网端口列表。端口之间需用逗号隔开（逗号前后不能有空格）；连续的一组端口可以用"-"符号表示，如 1-10 表示端口 1 到 10；组与组之间用逗号隔开。

模式

全局配置模式

说明

在 interface range 配置模式下，同一命令会作用到列表中的所有端口上。但各个端口是相互独立的，如果命令在一个端口上执行失败，不会影响其他端口上的执行。

示例

进入接口配置模式，并将以太网端口 1,2,3,6,7,8,9 加入到一个端口组里，对它们同时进行配置：

TP-LINK(config)# interface range ethernet 1-3,6-9

22.3 description

该命令用于设置端口描述，它的 no 命令用于清空相应端口的描述。

命令

description *string*

no description

参数

string —— 端口描述的内容，可输入 1~16 个字符。

模式

接口配置模式（interface ethernet）

示例

为端口 5 添加端口描述 Port #5：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# description Port #5

22.4 shutdown

该命令用于禁用以太网端口，它的 no 命令用于重新启用相应端口。

命令

shutdown

no shutdown

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

关闭以太网端口 3：

TP-LINK(config)# interface ethernet 3

TP-LINK(config-if)# shutdown

22.5 flow-control

该命令用于启用端口的流量控制，它的 no 命令用于禁用相应端口的流控。启用流控能够同步接收端和发送端的速率，防止因速率不一致而导致的网络丢包。

命令

flow-control

no flow-control

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启以太网端口 5 的流量控制：

```
TP-LINK(config)# interface ethernet 5
TP-LINK(config-if)# flow-control
```

22.6 negotiation

该命令用于设置端口的协商模式，它的 no 命令用于恢复默认设置。

命令

negotiation { auto | 10h |10f |100h |100f |1000f }

no negotiation

参数

auto | 10h |10f |100h |100f |1000f —— 端口协商模式，分别为自协商模式、10M 半双工、10M 全双工、100M 半双工、100M 全双工、1000M 全双工。缺省时为 auto。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置以太网端口 5 的协商模式为 100M 全双工：

```
TP-LINK(config)# interface ethernet 5
TP-LINK(config-if)# negotiation 100f
```

22.7 storm-control

该命令用于配置风暴抑制，它的 no 命令用于禁用风暴抑制。风暴抑制是允许交换机对网络上出现的广播包、组播包和 UL 包进行过滤。当交换机发现这三种包超出您设定的最大速率时，会自动丢弃，以防止网络广播风暴的发生。

命令

storm-control [**bc-rate** *bc-rate*] [**mc-rate** *mc-rate*] [**ul-rate** *ul-rate*]

no storm-control

参数

bc-rate —— 广播包抑制，即广播包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 100k | 200k | 500k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

mc-rate —— 组播包抑制，即组播包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 100k | 200k | 500k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

ul-rate —— UL 包抑制，即 UL 包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 100k | 200k | 500k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 5 的风暴抑制，其中广播包抑制速率为 100kbps，组播包为 500kbps，UL 包为 2Mbps：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# storm-control bc-rate 100k **mc-rate** 500k **ul-rate** 2m

22.8 storm-control disable bc-rate

该命令用于单独禁用广播包抑制。

命令

storm-control disable bc-rate

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

禁用端口 5 的广播包抑制：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# storm-control disable bc-rate

22.9 storm-control disable mc-rate

该命令用于单独禁用组播包抑制。

命令

storm-control disable mc-rate

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

禁用端口 5 的组播包抑制：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# storm-control disable mc-rate

22.10 storm-control disable ul-rate

该命令用于单独禁用 UL 包抑制。

命令

storm-control disable ul-rate

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

禁用端口 5 的 UL 包抑制：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# storm-control disable ul-rate

22.11 port rate-limit

该命令用于配置以太网端口的带宽限制，它的 no 命令用于禁用端口带宽限制。

命令

port rate-limit [**ingress** *ingress-rate*] [**egress** *egress-rate*]

no port rate-limit

参数

ingress-rate —— 配置入口带宽限制，单位为 bps，取值范围 100k | 200k | 500k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

egress-rate —— 配置出口带宽限制，单位为 bps，取值范围 100k | 200k | 500k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

配置端口 5 的入口带宽为 10Mbps，出口带宽为 1Mbps：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# port rate-limit ingress 10m **egress** 1m

22.12 port rate-limit disable ingress

该命令用于单独禁用入口带宽限制。

命令

port rate-limit disable ingress

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

禁用端口 5 的入口带宽限制：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# port rate-limit disable ingress

22.13 port rate-limit disable egress

该命令用于单独禁用出口带宽限制。

命令

port rate-limit disable egress

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

禁用端口 5 的出口带宽限制：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# port rate-limit disable egress

22.14 show interface configuration

该命令用于显示以太网端口的配置信息，包括端口状态、流量控制、协商模式和端口描述等。

命令

show interface configuration { **ethernet** [*interface*] }

参数

interface —— 要显示配置信息的以太网端口，缺省时显示所有端口的信息。

模式

所有命令模式

示例

显示以太网端口 5 的配置信息：

TP-LINK# show interface configuration ethernet 5

22.15 show interface status

该命令用于显示以太网端口的连接状态。

命令

show interface status { **ethernet** [*interface*] }

参数

Interface —— 要显示连接状态的以太网端口，缺省时显示所有端口的状态。

模式

所有命令模式

示例

显示所有以太网端口的连接状态：

TP-LINK(config)# show interface status ethernet

22.16 show interface counters

该命令用于显示以太网端口的统计信息。

命令

show interface counters { **ethernet** [*interface*] }

参数

Interface —— 要显示统计信息的以太网端口，缺省时显示所有端口的信息。

模式

所有命令模式

示例

显示以太网端口 3 的统计信息：

TP-LINK(config)# show interface counters ethernet 3

22.17 show storm-control ethernet

该命令用于显示接口的风暴抑制信息。

命令

show storm-control ethernet [*port*]

参数

port —— 要显示风暴抑制信息的端口号，取值范围 1~28，缺省时显示所有端口的风暴抑制信息。

模式

所有命令模式

示例

显示所有端口的风暴抑制信息：

```
TP-LINK(config)# show storm-control ethernet
```

22.18 show port rate-limit

该命令用于显示端口的带宽限制信息。

命令

show port rate-limit [*interface-num*]

参数

interface-num —— 要显示速率限制信息的端口号，取值范围 1~28，缺省时显示所有端口的速率限制信息。

模式

所有命令模式

示例

显示所有端口的速率限制信息：

```
TP-LINK(config)# show port rate-limit
```

第23章 QoS配置命令

QoS（Quality of Service，服务质量）功能用以提高网络传输的可靠性，提供更高质量的网络服务。

23.1 qos

该命令用于设置基于端口的 CoS，它的 no 命令用于恢复某端口的默认 CoS。

命令

qos *cos-id*

no qos

参数

cos-id —— 端口对应的优先级等级，可选范围为 0~7，表示 CoS0~CoS7。默认值为 0。

模式

接口配置模式（interface ethernet / interface range ehternet）

说明

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据端口的 CoS 值以及 IEEE 802.1P 中 CoS 到 TC 之间的映射关系来确定数据流的出口队列。

示例

设置端口 5 的优先级等级为 3：

```
TP-LINK(config)# interface ethernet 5
TP-LINK(config-if)# qos 3
```

23.2 qos dot1p enable

该命令用于用于启用 IEEE 802.1P 的优先级 tag 和出口队列的映射关系，它的 no 命令用于禁用这种关系。

命令

qos dot1p enable

no qos dot1p enable

模式

全局配置模式

示例

启用优先级 tag 和出口队列的映射关系：

```
TP-LINK(config)# qos dot1p enable
```

23.3 qos dot1p config

该命令用于设置 IEEE 802.1P 的优先级 tag 和出口队列的映射关系，它的 no 命令用于恢复默认设置。IEEE 802.1P 对 IEEE 802.1Q tag 中的 Pri 字段给予了推荐性的定义，利用该字段可以将数据包划分为 8 个优先级。启用 IEEE 802.1P 优先级后，交换机根据数据包是否带有 IEEE 802.1Q tag 来确定所使用的优先级模式。对于带有 tag 的数据包，应用 IEEE 802.1P 优先级，否则应用基于端口的优先级。

命令

qos dot1p config {*tag*} {*cos-id*}

no qos dot1p config

参数

tag —— IEEE 802.1P 协议里规定的 8 个优先级，取值范围是 0~7。

cos-id —— tag 对应的优先级等级，可选范围为 0~3，分别对应 4 个不同等级的出口队列 TC0~TC3。

模式

全局配置模式

说明

1. 默认情况下，tag 和出口队列的对应关系是：
   0-TC1，1-TC0，2-TC0，3-TC1，4-TC2，5-TC2，6-TC3，7-TC3。
2. 优先级等级 TC0、TC1...TC3 中，数字越大，表示优先级越高。

示例

设置 tag 优先级 0 的对应出口队列优先级为 TC3：

```
TP-LINK(config)# qos dot1p config 0 3
```

23.4 qos dscp enable

该命令用于启用 DSCP 优先级的 DSCP 值和出口队列的映射关系，它的 no 命令用于禁用该映射关系。

命令

qos dscp enable

no qos dscp enable

模式

全局配置模式

示例

启用 DSCP 优先级的 DSCP 值和出口队列的映射关系：

```
TP-LINK(config)# qos dscp enable
```

23.5 qos dscp config

该命令用于设置 DSCP 优先级的 DSCP 值和出口队列的映射关系，它的 no 命令用于恢复默认设置。DSCP（DiffServ Code Point，区分服务编码点）是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。启用 DSCP 优先级后，如果转发的数据包是 IP 报文，则交换机应用 DSCP 优先级；如果是非 IP 报文，交换机则根据是否启用了 IEEE 802.1P 优先级以及数据帧是否带有 tag 来决定采用哪种优先级模式。

命令

qos dscp config {*dscp-list*} {*cos-id*}

no qos dscp config

参数

dscp-list —— DSCP 值列表，可选择一个或多个 DSCP 值，连续的一组 DSCP 值可以用"-"符号表示，不连续的值之间、不同组之间需用逗号隔开，如 1,4-7,11 表示选择 1,4,5,6,7,11。DSCP 值的可选范围为 0~63。

cos-id —— DSCP 值对应的优先级等级，可选范围为 0~3，分别对应 4 个不同等级的出口队列 TC0~TC3。

模式

全局配置模式

说明

1. 默认情况下，DSCP 值 0-15 对应等级 TC0，DSCP 值 16-31 对应等级 TC1，DSCP 值 32-47 对应等级 TC2，DSCP 值 48-63 对应等级 TC3。
2. 优先级等级 TC0、TC1…TC3 中，数字越大，表示优先级越高。

示例

设置 DSCP 值 10,11,15 对应的出口队列优先级为 TC0：

```
TP-LINK(config)# qos dscp config 10,11,15 0
```

23.6 qos scheduler

该命令用于设置出口队列调度模式，它的 no 命令用于恢复默认配置。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法

来控制报文的转发次序。本交换机以 TC0、TC1…TC3 表示不同的优先级队列。

命令

qos scheduler { sp | wrr | sp+wrr | equ }

no qos scheduler

参数

sp —— 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。

wrr —— 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0 到 TC3 的权重比值是 1：2：4：8。

sp+wrr —— sp 和 wrr 的混合模式。在此模式下，交换机提供了 sp 和 wrr 两个调度组，其中 sp 组和 wrr 组之间遵循的是严格优先级调度规则，而 wrr 组内部队列遵循的是 wrr 调度规则。在该调度模式下，TC3 属于 sp 组；TC0、TC1 和 TC2 属于 wrr 组，权重比是 1：2：4。这样在调度的时候首先是 TC3 按照 sp 的调度模式独自占用带宽，然后是 wrr 组的成员 TC0、TC1 和 TC2 按照权重比 1：2：4 的比例占用带宽。

equ —— 无优先级模式，默认选项。在此模式下所有的队列公平地占用带宽，所有队列的权重比是 1：1：1：1。

模式

全局配置模式

示例

设置出口队列的调度模式为加权轮询优先级模式：

TP-LINK(config)# qos scheduler wrr

23.7 show qos port-based

该命令用于显示基于端口优先级的配置信息。

命令

show qos port-based [*interface-num*]

参数

interface-num —— 要显示基于端口优先级配置信息的以太网端口号，取值范围 1~28，缺省时显示所有端口的信息。

模式

所有命令模式

示例

显示以太网端口 5 的 QoS 配置信息：

```
TP-LINK# show qos port-based 5
```

23.8 show qos dot1p

该命令用于显示 IEEE 802.1P 优先级的配置信息。

命令

show qos dot1p

模式

所有命令模式

示例

显示 IEEE 802.1P 优先级的配置信息：

```
TP-LINK# show qos dot1p
```

23.9 show qos dscp

该命令用于显示 DSCP 优先级的配置信息。

命令

show qos dscp

模式

所有命令模式

示例

显示 DSCP 优先级的配置信息：

```
TP-LINK# show qos dscp
```

23.10 show qos scheduler

该命令用于显示出口队列的调度规则。

命令

show qos scheduler

模式

所有命令模式

示例

显示出口队列的调度规则：

```
TP-LINK# show qos scheduler
```

第24章 端口监控配置命令

端口监控是将被监控端口的报文复制到监控端口，在监控端口接入数据分析设备，利用该设备分析经过监控端口的报文，达到网络监控和故障排除的目的。

24.1 port mirror

该命令用于启用端口监控功能，它的 no 命令用于禁用端口监控。

命令

port mirror

no port mirror

模式

接口配置模式（interface ethernet）

示例

设置端口 1 为监控端口：

```
TP-LINK(config)# interface ethernet 1
TP-LINK(config-if)# port mirror
```

24.2 port mirrored

该命令用于设置端口监控，它的 no 命令用于删除相应设置。

命令

port mirrored {*port-list*} { ingress | egress | both }

no port mirrored {*port-list*} { ingress | egress | both }

参数

port-list —— 被监控端口列表，可选择一个或多个端口，输入格式为 1,2-4。

ingress —— 只对被监控端口收到的数据进行监控，即入口监控。

egress —— 只对被监控端口发出的数据进行监控，即出口监控。

both —— 同时监控被监控端口收到和发出的数据，即出、入口监控。

模式

接口配置模式（interface ethernet / interface range ehternet）

说明

1. 监控端口即为当前接口配置模式所对应的端口。

2. 被监控端口个数不做限制，但它不可以同时为监控端口。
3. 监控端口和被监控端口可以处于同一 VLAN 中，也可以不处于同一 VLAN 中。
4. 监控端口和被监控端口不能为汇聚端口成员。

示例

由端口 1 监控端口 2,5,6,7,9 的输入数据：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# port mirror

TP-LINK(config-if)# port mirrored 2,5-7,9 ingress

24.3 show port mirror

该命令用于显示端口监控配置信息。

命令

show port mirror

模式

所有命令模式

示例

显示当前的端口监控配置信息：

TP-LINK# show port mirror

第25章 ACL配置命令

ACL（Access Control List，访问控制列表），通过配置匹配规则、处理操作以及时间权限来实现对数据包的过滤，提供灵活的安全访问控制策略，为控制网络安全提供方便。

25.1 acl time-segment

该命令用于添加时间段，它的 no 命令用于删除对应的时间段。当用户配置的 ACL 规则需要按时间段进行过滤时，可以先配置时间段，然后在相应的规则下通过时间段名称引用该时间段，这条规则只在该指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

命令

acl time-segment {*name*} [**start-time** *start-time*] [**end-time** *end-time*] [**week-day** *week-day*] [**start-date** *start-date*] [**end-date** *end-date*] [**holiday** { disable | enable }]

no acl time-segment {*name*}

参数

name —— 要添加的时间段名称，可输入 1~16 个字符。

start-time —— 时间片段的起始时间，形式为 HH:MM，缺省时为 00：00。

end-time —— 时间片段的结束时间，形式为 HH:MM，缺省时为 23：59。

week-day —— 周期模式，形式为 1-3，6，也可输入 daily，off-day，working-day。其中 1-3，6 表示周一、周二、周三和周六；daily 表示每天，即周一到周日；off-day 表示周末，即周六和周日；working-day 表示工作日，即周一到周五。缺省时禁止周期模式。

start-date —— 绝对模式下的起始日期，形式为 MM/DD/YYYY，缺省时为 01/01/1970。

end-date —— 绝对模式下的结束日期，形式为 MM/DD/YYYY，缺省时为 12/31/2099。若起始日期和结束日期同时缺省，则禁止绝对模式。

holiday —— 是否启用假期模式，缺省时为禁用（disable）。

模式

全局配置模式

示例

添加一个名为 tSeg1 的时间段，时间范围为工作日的 8：30~12：00：

TP-LINK(config)# acl time-segment tSeg1 **start-time** 08:30 **end-time** 12:00 **week-day** working-day

25.2 acl holiday

该命令用于创建 **acl time-segment** 假期模式的节假日，它的 no 命令用于删除相应节假日。

命令

acl holiday {*name*} {*start-date*} {*end-date*}

no acl holiday {*name*}

参数

name —— 节假日名称，可输入 1~16 个字符。

start-date —— 节假日的起始日期，格式为 MM/DD，如 05/01。

end-date —— 节假日的结束日期，格式为 MM/DD，如 05/03。

模式

全局配置模式

示例

定义节假日国庆节，并设置其起止时间为 10 月 1 日到 10 月 3 日：

```
TP-LINK(config)# acl holiday NationalDay 10/01 10/03
```

25.3 acl create

该命令用于创建 ACL，它的 no 命令用于删除对应的 ACL 条目。

命令

acl create *id*

no acl create *id*

参数

id —— ACL ID 号，0-99 为 MAC 访问控制列表，100-199 为标准 IP 访问控制列表，200-299 为扩展 IP 访问控制列表。

模式

全局配置模式

示例

创建一个 ID 号为 20 的 MAC ACL：

```
TP-LINK(config)# acl create 20
```

25.4 acl rule mac-acl

该命令用于添加 MAC ACL 规则，它的 no 命令用于删除对应规则。MAC ACL 根据数据包的源 MAC

地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

命令

acl rule mac-acl {*acl-id*} {*rule-id*} [**op** { discard | permit }] [[**smac** *source-mac*] {**smask** *source-mac-mask*}] [[**dmac** *destination-mac*] {**dmask** *destination-mac-mask*}] [**vid** *vlan-id*] [**type** *ethernet-type*] [**pri** *user-pri*] [**tseg** *time-segment*]

no acl rule mac-acl {*acl-id*} {*rule-id*}

参数

acl-id —— 要添加规则的 ACL ID 号。

rule-id —— 当前添加的规则的 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 discard 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

source-mac —— 规则包含的源 MAC 地址。

source-mac-mask —— 源 MAC 地址的掩码。若您输入了源 MAC 地址，则必须输入相应的掩码。

destination-mac —— 规则包含的目的 MAC 地址。

destination-mac-mask —— 目的 MAC 地址的掩码。若您输入了目的 MAC 地址，则必须输入相应的掩码。

vlan-id —— 规则包含的 VLAN ID 号，取值范围为 1~4094。

ethernet-type —— 规则包含的以太网类型信息，输入格式为 4 位 16 进制数。

user-pri —— 用户优先级，取值范围为 0~7，缺省时为无限制。

time-segment —— 规则生效的时间段的名称，缺省时为无限制。

模式

全局配置模式

示例

创建一个 ID 号为 20 的 MAC ACL，为其添加规则 10，其中源 MAC 地址为 00:01:3F:48:16:23，掩码为 11:11:11:11:11:00，VLAN ID 为 2，用户优先级为 5，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

TP-LINK(config)# acl create 20

TP-LINK(config)# acl rule mac-acl 20 10 **op** permit **smac** 00:01:3F:48:16:23 **smask** 11:11:11:11:11:00 **vid** 2 **pri** 5 **tseg** tSeg1

25.5 acl rule std-acl

该命令用于添加标准 IP ACL 规则，它的 no 命令用于删除对应规则。标准 IP ACL 可以根据数据包的 IP 地址信息制定匹配规则，对数据包进行相应的分析处理。

命令

acl rule std-acl {*acl-id*} {*rule-id*} [**op** { discard | permit }] [[**sip** *source-ip*] {**smask** *source-ip-mask*}] [[**dip** *destination-ip*] {**dmask** *destination-ip-mask*}] [**tseg** *time-segment*] [**frag** { disable | enable }]

no acl rule std-acl {*acl-id*} {*rule-id*}

参数

acl-id —— 要添加规则的 ACL ID 号。

rule-id —— 当前添加的规则的 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 discard 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

source-ip —— 规则包含的源 IP 地址。

source-ip-mask —— 源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip —— 规则包含的目的 IP 地址。

destination-ip-mask —— 目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

time-segment —— 规则生效的时间段的名称，缺省时为无限制。

frag —— 是否启用分片报文，缺省时为禁用（disable）。启用分片报文时，此规则对所有分片报文进行处理，而最后一片报文总是允许转发。

模式

全局配置模式

示例

创建一个 ID 号为 120 的标准 IP ACL，为其添加规则 10，其中目的 IP 地址为 192.168.0.100，掩码为 255.255.255.0，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

TP-LINK(config)# acl create 120

TP-LINK(config)# acl rule std-acl 120 10 **op** permit **dip** 192.168.0.100 **dmask** 255.255.255.0 **tseg** tSeg1

25.6 acl policy policy-add

该命令用于添加 Policy，它的 no 命令用于删除对应的 Policy 条目。Policy 功能将 ACL 和动作组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，添加的操作包括流镜像、流监控、QoS Remarking 和端口重定向。

命令

acl policy policy-add *name*

no acl policy policy-add *name*

参数

name —— 要添加的 Policy 名称，可输入 1~16 个字符。

模式

全局配置模式

示例

添加一个名为 policy1 的 Policy：

TP-LINK(config)# acl policy policy-add policy1

25.7 acl policy action-add

该命令用于为 Policy 添加 ACL 并设置动作，它的 no 命令用于删除相应动作。

命令

acl policy action-add {*policy-name*} {*acl-id*} [**rate** *rate*] [**osd** { none | discard }] [**e-port** *egress-port*] [**vid** *vlan-id*] [**dscp** *dscp*] [**pri** *local-pri*] [**mirr** *mirror*]

no acl policy action-add {*policy-name*} {*acl-id*}

参数

policy-name —— 要设置的 Policy 的名称。

acl-id —— Policy 作用的 ACL 的 ID 号。

rate —— 流监管的额定速率，取值范围为 1~1000000（kbps）。

osd —— 流监管的超速处理，即对超过额定速率的数据包的处理方式，有不处理（none）和丢弃（discard）两个选项。缺省时为不处理。

egress-port —— 端口重定向的出口端口，即将匹配了相应 ACL 的数据包指定到此处所设的端口转发。取值范围为 1~28，缺省时为所有端口。

vlan-id —— 端口重定向的 VLAN ID 号，即将匹配了相应 ACL 的数据包指定在此处所设的 VLAN 中转发。取值范围为 1~4094。

dscp —— QoS 重标记之 DSCP，为匹配了相应 ACL 的数据包指定 DSCP 域。取值范围

为 0~63，缺省时为无限制。

local-pri —— QoS 重标记之本地优先级，为匹配了相应 ACL 的数据包指定优先级。取值范围为 0~3。

mirror —— 流镜像的镜像端口。取值范围为 1~28，缺省时为 1。

模式

全局配置模式

示例

创建一个名为 policy1 的 Policy，对符合 ACL 120 相应规则的数据包，若速率超过 1000kbps，交换机将予以丢弃：

TP-LINK(config)# acl policy policy-add policy1

TP-LINK(config)# acl policy action-add policy1 120 **rate** 1000 **osd** discard

25.8 acl bind to-port

该命令用于绑定 Policy 到指定端口，它的 no 命令用于取消绑定。

命令

acl bind to-port {*policy-name*} {*port*}

no acl bind to-port {*policy-name*} {*port*}

参数

policy-name —— 要绑定到端口的 Policy 名称。

port —— 要绑定的端口号，取值范围 1~28。

模式

全局配置模式

示例

将 policy1 绑定到端口 1：

TP-LINK(config)# acl bind to-port policy1 1

25.9 acl bind to-vlan

该命令用于绑定 Policy 到指定 VLAN，它的 no 命令用于取消绑定。

命令

acl bind to-vlan {*policy-name*} {*vlan-id*}

no policy to-vlan {*policy-name*} {*vlan-id*}

参数

policy-name —— 要绑定到 VLAN 的 Policy 名称。

vlan-id —— 要绑定的 VLAN 的 VLAN ID，取值范围 1~4094。

模式

全局配置模式

示例

将 policy1 绑定到 VLAN 2：

TP-LINK(config)# acl bind to-vlan policy1 2

25.10 show acl time-segment

该命令用于显示所有时间段的配置。

命令

show acl time-segment

模式

所有命令模式

示例

显示所有时间段配置：

TP-LINK> show acl time-segment

25.11 show acl holiday

该命令用于显示所有已定义的节假日。

命令

show acl holiday

模式

所有命令模式

示例

显示节假日设置：

TP-LINK> show acl holiday

25.12 show acl config

该命令用于显示 ACL 配置。

命令

show acl config *acl-id*

参数

acl-id —— 要显示配置的 ACL ID 号。

模式

所有命令模式

示例

显示 ID 号为 20 的 MAC ACL 的配置：

TP-LINK> show acl config 20

25.13 show acl bind

该命令用于显示 Policy 绑定配置。

命令

show acl bind

模式

所有命令模式

示例

显示 Policy 绑定设置：

TP-LINK> show acl bind

第26章 MSTP配置命令

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 IEEE 802.1S 标准建立的，用于在局域网中消除数据链路层物理环路的协议。生成树协议的基本思想是通过构造一棵或多棵自然树的方法达到裁剪冗余环路的目的，同时实现链路备份和路径最优化。

26.1 spanning-tree global

该命令用于生成树协议全局配置，它的 no 命令用于恢复默认配置。

命令

spanning-tree global [**state** { disable | enable }] [**mode** { stp | rstp | mstp }] [**cist** *cist*] [**htime** *hello-time*] [**mage** *max-age*] [**delay** *forward-delay*] [**hcount** *hold-count*] [**mhop** *max-hops*]

no spanning-tree global

参数

state —— 选择是否启用交换机的生成树功能，缺省时为禁用（disable）。

mode —— 生成树模式，有 STP、RSTP、MSTP 三个选项，默认为 STP。其中 STP 为生成树兼容模式；RSTP 为快速生成树兼容模式；MSTP 为多重生成树模式。

cist —— 交换机的 CIST 优先级，范围 0~61440，间隔 4096，缺省时为 32768。CIST 优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。值越小，表示优先级越高。

hello-time —— 联络时间，即交换机发送协议报文的周期，用于检测链路是否存在故障，取值范围为 1~10（秒），默认值为 2，并且 2×（联络时间+1）≤老化时间。

max-age —— 老化时间，即协议报文在交换机中能够保存的最大生命期，取值范围为 6~40（秒），默认值为 20。

forward-delay —— 传输延时，即在网络拓扑改变后，交换机的端口状态迁移的延时时间，取值范围为 4~30（秒），默认值为 15，并且 2×（传输延时-1）≥老化时间。

hold-count —— 流量限制，即在每个联络时间内，端口最多能够发送的协议报文的速度。取值范围为 1~20（pps），默认值为 5。

max-hops —— 最大跳数，即协议报文被转发的最大跳数，它限制了生成树的规模，取值范围为 1~40（跳），默认值为 20。

模式

全局配置模式

示例

开启交换机的生成树功能，并设置生成树模式为 MSTP，CIST 优先级为 4096，联络时间为 4 秒，老化时间为 10 秒，传输延时为 10 秒，流量限制为 8pps，最大跳数为 15：

TP-LINK(config)# spanning-tree global state enable **mode** mstp **cist** 4096 **htime** 4 **mage** 10 **delay** 10 **hcount** 8 **mhop** 15

26.2 spanning-tree common-config

该命令用于生成树协议端口配置，它的 no 命令用于恢复默认配置。CIST（Common and Internal Spanning Tree，公共和内部生成树）是连接一个交换网络内所有设备的单生成树。本命令用来配置端口基于 CIST 的参数以及所有实例的共用参数。

命令

spanning-tree common-config [**enable** { disable | enable }] [**pri** *priority*] [**expath** *expath-consum*] [**inpath** *inpath-consum*] [**edge** { disable | enable }] [**ptop** { auto | open | close }]

no spanning-tree common-config

参数

enable —— 端口是否启用 STP 功能，缺省时为禁用（disable）。

priority —— 优先级，它是确定端口是否会被对端设备选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。取值范围 0~240，间隔 16，缺省时为 128。

expath-consum —— 外部路径开销。它是在不同 MST 域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

inpaht-consum —— 内部路径开销。它是在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

edge —— 是否启用边缘端口，缺省时为禁用（disable）。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

ptop —— 点对点链路状态，有自动（auto）、强制开启（open）和强制关闭（close）三个选项，缺省时为自动。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 1 的 STP 功能，并设置其优先级为 64，内、外部路径开销均为 100，开启边缘端口：

TP-LINK(config)# interface ethernet 1

TP-LINK(config-if)# spanning-tree common-config enable enable **pri** 64 **expath** 100 **inpath** 100 **edge** enable

26.3 spanning-tree region

该命令用于 MSTP 的域配置。MSTP 可以将交换网络划分为多个域，有着相同域配置和 VLAN-实例映射关系的交换机被认为属于同一个 MST 域（Multiple Spanning Tree Regions，多生成树域）。域配置包括配置域名和修订级别。

命令

spanning-tree region {*name*} {*revision*}

参数

name —— 域名，用于标识 MST 域，可输入 1~32 个字符。

revision —— 修订级别，范围为 0~65535。

模式

全局配置模式

示例

配置 MSTP 的域名为 r1，修订级别为 100：

TP-LINK(config)# spanning-tree region r1 100

26.4 spanning-tree msti

该命令用于 MSTP 实例配置，它的 no 命令用于恢复对应实例的默认配置。实例配置是 MST 域的一个属性，用来描述 VLAN 和生成树实例的映射关系。可以按需要分配 VLAN 属于不同的实例，每个实例就是一个“VLAN 组”，不受其他实例和公共生成树的影响。

命令

spannint-tree msti {*msti-id*} [**status** { disable | enable }] [**pri** *priority*] [**mapped** *mapped*]

no spanning-tree msti {*msti-id*}

参数

msti-id —— 实例 ID，范围为 1~8。

status —— 是否启用相应实例，缺省时为禁用（disable）。

priority —— MSTI 优先级，它是在对应实例 ID 中，确定交换机是否会被选为根桥的重要依据。取值范围 0~61440，间隔 4096，缺省时为 32768。

mapped —— VLAN-实例映射，输入要加入该实例的 VLAN ID，格式为 1,2-4。

模式

全局配置模式

示例

启用实例 1，并为其添加 VLAN 2、3、4、5、8，设置 MSTI 优先级为 4096：

TP-LINK(config)# spanning-tree msti 1 **status** enable **pri** 4096 **mapped** 2-5,8

26.5 spanning-tree msti

该命令用于 MSTP 实例端口配置，它的 no 命令用于恢复对应实例端口的默认配置。端口在不同的生成树实例中可以担任不同的角色，本命令用来配置不同实例 ID 中的端口的参数。

命令

spanning-tree msti {*id*} [**pri** *pri*] [**path** *path*]

no spanning-tree msti {*id*}

参数

id —— 需要配置端口属性的实例 ID 号，取值范围 1~8。

pri —— 端口优先级，它是在对应实例 ID 中，确定端口是否会被对端设备选为根端口的重要依据。取值范围 0~240，间隔 16，缺省时为 128。

path —— 路径开销。路径开销是在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

设置实例 1 的端口 5 优先级为 64，路径开销为 100：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# spanning-tree msti 1 **pri** 64 **path** 100

26.6 spanning-tree tc-defend

该命令用于配置生成树的全局 TC 保护，它的 no 命令用于恢复默认配置。设备在接收到 TC 报文（网络拓扑发生变化的通知报文）后，会执行地址表项的删除操作。当设备受到恶意的 TC 报文攻击时，

频繁地删除操作会给设备带来很大负担，给网络的稳定带来很大隐患。TC 保护可以限制一定周期内交换机接收 TC 报文的最大数目，从而控制地址表项的删除操作。

命令

spanning-tree tc-defend [**threshold** *threshold*] [**period** *period*]

no spanning-tree tc-defend

参数

threshold —— TC 保护阀值，取值范围 1~100（数据包），缺省时为 20。TC 保护阀值是在 TC 保护周期内，交换机收到 TC 报文的最大数目。超过该数目后，交换机在该周期内不再进行删除地址表的操作。

period ——TC 保护周期，取值范围 1~10（秒），缺省时为 5。

模式

全局配置模式

示例

设置 TC 保护阀值为 30 数据包，TC 保护周期为 10 秒：

TP-LINK(config)# spanning-tree tc-defend threshold 30 **period** 10

26.7 spanning-tree security

该命令用于配置 MSTP 端口保护，它的 no 命令用于恢复默认配置。端口保护功能可以防止 STP 协议网络中的设备遭受各种形式的恶意攻击。

命令

spanning-tree security [**loop** { disable | enable }] [**root** { disable | enable }] [**TC** { disable | enable }] [**defend** { disable | enable }] [**hold** { disable | enable }]

no spanning-tree security

参数

loop —— 是否启用环路保护，默认为禁用。环路保护可以防止由于链路拥塞或者单项链路故障，导致下游设备重新计算生成树，从而产生的网络环路现象。

root —— 是否启用根桥保护，默认为禁用。根桥保护可以防止当前合法根桥失去根桥地位，从而引起的网络拓扑结构的错误变动。

TC —— 是否启用 TC 保护，默认为禁用。

defend —— 是否启用 BPDU 保护，默认为禁用。BPDU 保护可以防止边缘端口受到恶意伪造的协议报文的攻击。

hold —— 是否启用 BPDU 过滤，默认为禁用。BPDU 过滤可以防止 STP 协议网络中的协议报文泛洪。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 2 的环路保护、根桥保护、TC 保护、BPDU 保护和 BPDU 过滤：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# spanning-tree security loop enable **root** enable **TC** enable **defend** enable **hold** enable

26.8 spanning-tree mcheck

该命令用于启用协议迁移。

命令

spanning-tree mcheck

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 2 的协议迁移：

TP-LINK(config)# interface ethernet 2

TP-LINK(config-if)# spanning-tree mcheck

26.9 show spanning-tree global-info

该命令用于显示生成树的当前运行状态信息。

命令

show spanning-tree global-info

模式

所有命令模式

示例

显示生成树当前运行状态信息：

TP-LINK# show spanning-tree global-info

26.10 show spanning-tree global-config

该命令用于显示生成树的全局配置信息。

命令

show spanning-tree global-config

模式

所有命令模式

示例

显示生成树全局配置信息：

```
TP-LINK# show spanning-tree global-config
```

26.11 show spanning-tree port-config

该命令用于显示生成树的端口配置信息。

命令

show spanning-tree port-config [*port*]

参数

port —— 要显示配置信息的端口号，取值范围 1~28，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示端口 5 的配置信息：

```
TP-LINK(config)# show spanning-tree port-config 5
```

26.12 show spanning-tree region

该命令用于显示 MSTP 的域配置信息。

命令

show spanning-tree region

模式

所有命令模式

示例

显示 MSTP 域配置信息：

```
TP-LINK(config)# show spanning-tree region
```

26.13 show spanning-tree msti config

该命令用于显示生成树的实例配置信息。

命令

show spanning-tree msti config {*id*}

参数

id —— 要显示配置信息的实例 ID，取值范围 1~8。

模式

所有命令模式

示例

显示实例 1 的配置信息：

```
TP-LINK(config)# show spanning-tree msti config 1
```

26.14 show spanning-tree msti port

该命令用于显示生成树的实例端口配置信息。

命令

show spanning-tree msti port {*id*} [*port*]

参数

id —— 实例 ID 号，取值范围 1~8。

port —— 端口号，取值范围 1~28，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示实例 1 的端口 5 的配置信息：

```
TP-LINK(config)# show spanning-tree msti port 1 5
```

26.15 show spanning-tree security tc-defend

该命令用于显示生成树的 TC 保护阈值和周期。

命令

show spanning-tree security tc-defend

模式

所有命令模式

示例

显示生成树的 TC 保护阈值和周期：

TP-LINK(config)# show spanning-tree security tc-defend

26.16 show spanning-tree security port-defend

该命令用于显示生成树的端口安全配置信息。

命令

show spanning-tree security port-defend [*port*]

参数

port —— 要显示端口安全配置信息的端口号，取值范围 1~28，缺省时显示所有端口的安全配置信息。

模式

所有命令模式

示例

显示端口 2 的端口安全配置信息：

TP-LINK(config)# show spanning-tree security port-defend 2

第27章 IGMP配置命令

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在交换机上的组播约束机制，用于管理和控制组播组。启用 IGMP 侦听功能可以有效地避免组播数据在网络中广播。

27.1 igmp global

该命令用于 IGMP 全局配置，它的 no 命令用于恢复默认配置。

命令

igmp global [**state** { disable | enable }] [**unknown-packet** { pass | discard }]

no igmp global

参数

state —— 是否启用交换机的 IGMP 侦听功能，缺省时为禁用。

unknown-packet —— 交换机对未知组播报文的处理方法，有通过（pass）或丢弃（discard）两种方式，默认为通过。

模式

全局配置模式

示例

开启 IGMP，并将未知组播报文的处理方式设为丢弃：

TP-LINK(config)# igmp global state enable **unknown-packet** discard

27.2 igmp config

该命令用于配置端口 IGMP 侦听和快速离开功能，它的 no 命令用于恢复默认配置。

命令

igmp config state {disable | enable} **fast-leave** {disable | enable}

no igmp config

参数

state —— 是否开启端口 IGMP 侦听功能。

fast-leave —— 是否开启快速离开功能。当端口启用快速离开功能后，交换机收到 IGMP 离开报文时，会直接将该端口从组播组中删除。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 5 的 IGMP 侦听和快速离开功能：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# igmp config state enable **fast-leave** enable

27.3 igmp vlan-config-add

该命令用于添加普通 VLAN 配置，它的 no 命令用于删除对应的 VLAN 配置。IGMP 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 IGMP 参数，本命令用于配置每个 VLAN 的 IGMP 侦听参数。

命令

igmp vlan-config-add {*vlan-id*} [**rtime** *router-time*] [**mtime** *member-time*] [**ltime** *leave-time*] [**rport** *router-port*]

no igmp vlan-config-add {*vlan-id*}

参数

vlan-id —— 启用 IGMP 侦听功能的 VLAN ID，取值范围 1~4094。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 300。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 260。

leave-time —— 离开滞后时间，即主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围 1~30（秒），默认值为 1。

router-port —— 静态路由端口，多用于拓扑稳定的网络中，范围为 1~28。

模式

全局配置模式

示例

启用 VLAN 1 的 IGMP 侦听功能，并设置路由器端口时间为 200 秒、成员端口时间为 100 秒、离开滞后时间为 10 秒、静态路由端口为 1：

TP-LINK(config)# igmp vlan-config-add 1 **rtime** 200 **mtime** 100 **ltime** 10 **rport** 1

27.4 igmp vlan-config

该命令用于修改普通 VLAN 配置，它的 no 命令用于恢复对应 VLAN 的原有配置。

命令

igmp vlan-config {*vlan-id*} [**rtime** *router-time*] [**mtime** *member-time*] [**ltime** *leave-time*] [**rport** *router-port*]

no igmp vlan-config {*vlan-id*}

参数

vlan-id —— 要修改配置的 VLAN ID，取值范围 1~4094。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 300。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 260。

leave-time —— 离开滞后时间，即主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围 1~30（秒），默认值为 1。

router-port —— 静态路由端口，多用于拓扑稳定的网络中，范围为 1~28。

模式

全局配置模式

示例

修改 VLAN 1 的路由器端口时间为 300 秒、成员端口时间为 200 秒、离开滞后时间为 15 秒：

TP-LINK(config)# igmp vlan-config 1 **rtime** 300 **mtime** 200 **ltime** 15

27.5 igmp multi-vlan-config

该命令用于建立组播 VLAN，它的 no 命令用于删除对应的组播 VLAN。

命令

igmp multi-vlan-config { disable | enable } {*vid*} [**rtime** *router-time*] [**mtime** *member-time*] [**ltime** *leave-time*] [**rport** *router-port*]

no igmp multi-vlan-config

参数

disable | enable —— 是否启用组播 VLAN。

vid —— 要修改配置的 VLAN ID，取值范围 2~4094。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 300。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 260。

leave-time —— 离开滞后时间，即从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围 1~30（秒），默认值为 1。

router-port —— 静态路由端口，多用于拓扑稳定的网络中，范围为 1~28。

模式

全局配置模式

示例

开启组播 VLAN 功能，并设置 VLAN 2 的路由器端口时间为 300 秒、成员端口时间为 200 秒、离开滞后时间为 15 秒：

TP-LINK(config)# igmp multi-vlan-config enable 2 **rtime** 300 **mtime** 200 **ltime** 15

27.6 igmp static-entry-add

该命令用于添加组播的静态地址条目，它的 no 命令用于删除对应条目。通过此命令配置的组播组不是通过 IGMP 侦听学习到的，不受动态组播组及组播过滤的影响。组播地址范围为 224.0.0.0~239.255.255.255，可以加入的有效组播地址范围为 224.0.1.0~239.255.255.255。

命令

igmp static-entry-add {*ip*} {*vlan-id*} {*switch-port*}

no igmp static-entry-add {*ip*} {*vlan-id*}

参数

ip —— 静态绑定的组播 IP 地址。

vlan-id —— 组播 IP 对应的 VLAN ID，取值范围 1~4094。

switch-port —— 组播 IP 的转发端口，格式为 1-3,6,23。

模式

全局配置模式

示例

添加组播静态地址 225.0.0.1，此地址对应 VLAN 2，转发端口为端口 3：

TP-LINK(config)# igmp static-entry-add 225.0.0.1 2 3

27.7 igmp filter-add

该命令用于添加需要过滤的组播地址段，它的 no 命令用于删除对应的过滤地址。在启用了 IGMP 侦听功能后，可以通过配置组播过滤来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。组播地址范围为 224.0.0.0~239.255.255.255，可以加入的有效组播地址范围为 224.0.1.0~239.255.255.255。

命令

igmp filter-add {*id*} {*start-ip*} {*end-ip*}

no igmp filter-add {*id*}

参数

id —— 过滤地址 ID，范围为 1~30。

start-ip —— 过滤地址段的起始组播 IP 地址。

end-ip —— 过滤地址段的结束组播 IP 地址。

模式

全局配置模式

示例

添加过滤地址段 225.0.0.1~225.0.0.4，过滤地址 ID 为 20：

TP-LINK(config)# igmp filter-add 20 225.0.0.1 225.0.0.4

27.8 igmp filter-config

该命令用于修改组播过滤地址。

命令

igmp filter-config {*id*} {*start-ip*} {*end-ip*}

参数

id —— 过滤地址 ID，范围为 1~30。

start-ip —— 过滤地址段的起始组播 IP 地址。

end-ip —— 过滤地址段的结束组播 IP 地址。

模式

全局配置模式

示例

修改 ID 号为 20 的过滤地址段为 225.0.0.10~225.0.0.12：

TP-LINK(config)# igmp filter- config 20 225.0.0.10 225.0.0.12

27.9 igmp filter

该命令用于配置端口过滤，它的 no 命令用于恢复默认配置。当端口发送 IGMP 报告报文时，交换机会根据报文检查端口上配置的组播过滤地址 ID，如果组播地址未被过滤，则将这个端口加入到该组播组的转发端口列表中，否则交换机就会丢弃该 IGMP 报告报文，从而控制了用户所能加入的组播组。

命令

igmp filter [**state** [disable | enable] | **mode** [refuse | accept] | **addr-id** [*filter-addr-id*] | **maxgroup** [*max-group*]]

no igmp filter

参数

state —— 是否启用端口组播过滤功能，缺省时为禁用。

mode —— 动作模式，拒绝或允许。若为拒绝，则只处理组播地址不在过滤地址范围内的组播报文；若为允许，则只有组播地址属于过滤地址范围时，才处理组播报文。缺省时为允许。

filter-addr-id —— 该端口需要绑定的过滤地址 ID 号，格式为 1-3，4，6。一个端口最多只能绑定 5 个过滤地址 ID。

max-group —— 最多加入组播数。通过限制端口的最多加入组播组数，来避免某些端口占据过多带宽。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

开启端口 5 的组播过滤功能，并设置动作模式为允许，绑定过滤地址 2、3、4，最多加入组播数为 128：

TP-LINK(config)# interface ethernet 5

TP-LINK(config-if)# igmp filter state enable **mode** accept **addr-id** 2-4 **maxgroup** 128

27.10 show igmp global-config

该命令用于显示 IGMP 全局配置信息。

命令

show igmp global-config

模式

所有命令模式

示例

显示 IGMP 全局配置信息：

TP-LINK> show igmp global-config

27.11 show igmp port-config

该命令用于显示 IGMP 端口配置信息。

命令

show igmp port-config [*port*]

参数

port —— 要显示配置信息的端口号，取值范围 1~28，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示端口 2 的 IGMP 配置信息：

TP-LINK> show igmp global-config 2

27.12 show igmp vlan-config

该命令用于显示 IGMP VLAN 配置信息。

命令

show igmp vlan-config

模式

所有命令模式

示例

显示 IGMP VLAN 配置信息：

TP-LINK> show igmp vlan-config

27.13 show igmp multi-vlan

该命令用于显示组播 VLAN 配置信息。

命令

show igmp multi-vlan

模式

所有命令模式

示例

显示组播 VLAN 配置信息：

```
TP-LINK> show igmp multi-vlan
```

27.14 show igmp multi-ip-list

该命令用于显示组播 IP 列表。

命令

show igmp multi-ip-list

模式

所有命令模式

示例

显示组播 IP 列表：

```
TP-LINK> show igmp multi-ip-list
```

27.15 show igmp filter-ip-addr

该命令用于显示组播过滤地址表。

命令

show igmp filter-ip-addr

模式

所有命令模式

示例

显示组播过滤地址表：

```
TP-LINK(config)# show igmp filter-ip-addr
```

27.16 show igmp port-filter

该命令用于显示组播端口过滤配置信息。

命令

show igmp port-filter [*port-num*]

参数

port-num —— 要显示组播过滤配置信息的端口号，取值范围 1~28，缺省时显示所有端口的配置信息。

模式

所有命令模式

示例

显示端口 5 的组播过滤配置信息：

TP-LINK> show igmp port-filter 5

27.17 show igmp packet-stat

该命令用于显示所有端口的报文统计信息。

命令

show igmp packet-stat

模式

所有命令模式

示例

显示报文统计信息：

TP-LINK> show igmp packet-stat

27.18 show igmp packet-stat-clear

该命令用于清除所有端口的报文统计信息。

命令

show igmp packet-stat-clear

模式

所有命令模式

示例

清除报文统计信息：

TP-LINK> show igmp packet-stat-clear

第28章 SNMP配置命令

SNMP（Simple Network Management Protocol，简单网络管理协议）功能用于管理网络设备，实现与众多产品的无障碍连接，以便于网络管理员对网络节点的监控和操作。

28.1 snmp global

该命令用于 SNMP 全局配置，它的 no 命令用于恢复默认配置。

命令

snmp global [**enable** { disable | enable }] [**engine-id** *engine-id*] [**remote-id** *remote-id*]

no snmp global

参数

enable —— 是否启用交换机的 SNMP 功能，默认为禁用（disable）。

engine-id —— 本地引擎 ID，即本地 SNMP 实体的引擎 ID。本地用户建立在本地引擎之下。可输入 10~64 个十六进制字符，且字符个数必须是偶数。

remote-id —— 远程引擎 ID，即 SNMP 管理端的引擎 ID。远程用户建立在远程引擎之下。可输入 10~64 个十六进制字符，且字符个数必须是偶数。

模式

全局配置模式

示例

开启 SNMP 功能，配置本地引擎 ID 为 1234567890，远程引擎 ID 为 123456abcdef：

TP-LINK(config)# snmp global enable enable **engine-id** 1234567890 **remote-id** 123456abcdef

28.2 snmp view-add

该命令用于添加视图，它的 no 命令用于删除对应视图。在 SNMP 报文中使用管理变量（OID）来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。

命令

snmp view-add {*name*} {*mib-oid*} { include | exclude }

no snmp view-add {*name*} {*mib-oid*}

参数

name —— 要添加的视图条目的名称，可输入 1~16 个字符。一个视图可以有多个同名的视图条目。

mib-oid —— MIB 子树 OID，即该视图条目的管理变量（OID）。可输入 1~61 个字符。

include | exclude —— 视图类型，有包括（include）和排除（exclude）两个选项。选择包括时，该 OID 可以被管理软件管理；选择排除时，该 OID 不能被管理软件管理。

模式

全局配置模式

示例

添加视图 view1，并设置其 OID 为 1.3.6.1.6.3.20，该 OID 可以被管理软件管理：

TP-LINK(config)# snmp view-add view1 1.3.6.1.6.3.20 include

28.3 snmp group-add

该命令用于添加组管理配置，它的 no 命令用于删除对应的组。SNMP v3 提供了 VACM（View-based Access Control Model，基于视图的访问控制模型）及 USM（User-based Security Model，基于用户的安全模型）的认证机制。组内的用户通过读、写、通知视图来达到访问控制的目的。同时通过有无认证和有无加密等功能组合，为管理软件和被管理设备之间的通信提供更高的安全性。

命令

snmp group-add {*name*} [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**ro** *ro-view*] [**wo** *wo-view*] [**inform** *inform-view*]

no snmp group-add {*name*} {**smode** { v1 | v2c | v3 }} {**slev** { noAuthNoPriv | authNoPriv | authPriv }}

参数

name —— 要添加的组名，可输入 1~16 个字符。组名与“安全模式”和“安全级别”共同组成该组的标识，三项均相同才被认为是同一组。

smode —— 安全模式，有v1、v2c和v3 三个选项，分别表示SNMP v1、SNMP v2c和SNMP v3。其中SNMP v1 和SNMP v2c采用团体名（详见命令 **snmp community-add**）认证，SNMP v3 采用USM认证。缺省时为v1。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。SNMP v1 和 SNMP v2c 安全模式下不需设置此项。

ro-view —— 关联的只读视图名称。只读视图只能被查看不能被编辑。

wo-view —— 关联的只写视图名称。只写视图只能被编辑不能被查看。若要对某视图进行读写操作，则需同时将该视图添加为只读视图和只写视图。

inform-view —— 关联的通知视图名称。管理软件可以接收到通知视图发送的异常报警

信息。

模式

全局配置模式

示例

添加组 group1，并设置其安全模式为 SNMP v2c，组内的用户可对视图 view1 进行读写操作，管理软件可以接收到视图 view2 发送的异常报警信息：

TP-LINK(config)# snmp group-add group1 **smode** v2c **ro** view1 **wo** view1 **inform** view2

28.4 snmp user-add

该命令用于添加用户，它的 no 命令用于删除对应的用户。管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。

命令

snmp user-add {*name*} { local | remote } {*group-name*} [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**cmode** { none | MD5 | SHA }] [**cpwd** *confirm-pwd*] [**emode** { none | DES }] [**epwd** *encrypt-pwd*]

no snmp user-add {*name*}

参数

name —— 要添加的用户名，可输入 1~16 个字符。

local | remote —— 用户类型，分本地（local）和远程（remote）两种。本地用户即建立在本地引擎下的用户，远程用户即建立在远程引擎下的用户。

group-name —— 关联的组名。通过“组名”、“安全模式”和“安全级别”来确定用户所属的组。

smode —— 安全模式，有 v1、v2c 和 v3 三个选项，缺省时为 v1。用户的安全模式必须和其所属组的安全模式相同。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。用户的安全级别必须和其所属组的安全级别相同。

cmode —— SNMP v3 用户的认证模式，有 none、MD5 和 SHA 三个选项。其中 none 表示不认证；MD5 为信息摘要算法；SHA 为安全散列算法，比 MD5 的安全性更高。缺省时为 none。

confirm-pwd —— 认证密码，可输入 1~16 个字符。

emode —— SNMP v3 用户的加密模式，有 none 和 DES 两个选项。其中 none 表示不加密，DES 为数据加密标准。缺省时为 none。

encrypt-pwd —— 加密密码，可输入 1~16 个字符。

模式

全局配置模式

示例

将本地用户 admin 添加到组 group2，输入组的安全模式 v3、安全级别 authPriv，并设置用户的认证模式为 MD5、认证密码为 11111、加密模式为 DES、加密密码为 22222：

TP-LINK(config)# snmp user-add admin local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

28.5 snmp community-add

该命令用于添加团体，它的 no 命令用于删除对应的团体。SNMP v1 和 SNMP v2c 采用团体名（Community Name）认证，团体名起到了类似于密码的作用。

命令

snmp community-add {*name*} { read-only | read-write } {*mib-view*}

no snmp community-add {*name*}

参数

name —— 要添加的团体名称，可输入 1~16 个字符。

read-only | read-write —— 团体对相应视图的权限，有 read-only（只读）和 read-write（读写）两个选项。

mib-view —— MIB 视图，即团体可访问的视图。

模式

全局配置模式

示例

添加团体 community1，此团体对视图 view1 具有读写权限：

TP-LINK(config)# snmp community-add community1 read-write view1

28.6 snmp notify-add

该命令用于添加通知管理条目，它的 no 命令用于删除对应条目。通知管理功能是交换机主动向管理软件报告某些视图的重要事件，便于管理软件对交换机的某些事件进行及时监控和处理。

命令

snmp notify-add {*ip*} {*udp-port*} {*user-name*} [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform }] [**resend** *resend*]

[**timeout** *timeout*]

no snmp notify-add {*ip*} {*user-name*}

参数

ip —— 管理主机的 IP 地址。

udp-port —— UDP 端口号，即管理主机上开启供通知过程使用的 UDP 端口号，与 IP 地址共同作用。默认值为 162。

user-name —— 配置管理软件的团体名/用户名。

smode —— 用户的安全模式，有 v1、v2c 和 v3 三个选项。缺省时为 v1。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。

type —— 通知报文的类型，有 trap 和 inform 两个选项，缺省时为 trap。选择 trap 时，以 Trap 方式发送通知；选择 inform 时，以 Inform 方式发送通知。Inform 具有更高的可靠性，并且需要设置重传次数（resend）和超时时间（timeout）。v1 安全模式下只能选择 Trap 方式。

resend —— Inform 报文的重传次数，取值范围 1~255。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重发 Inform 报文。

timeout —— 超时时间，即交换机等待 Inform 回应报文的时间。超过该时间后，将重新发送 Inform 报文。取值范围为 1~3600（秒）。

模式

全局配置模式

示例

添加通知管理条目，其中管理主机的 IP 地址为 192.168.0.1，其 UDP 端口号为 162，管理软件的用户名为 admin，用户安全模式为 v2c，通知报文以 Inform 的方式发送，Inform 报文的超时时间为 1000 秒，重传次数 100 次：

TP-LINK(config)# snmp notify-add 192.168.0.1 162 admin **smode** v2c **type** inform **resend** 100 **timeout** 1000

28.7 snmp-rmon history sample-cfg

该命令用于配置历史采样条目，它的 no 命令用于恢复默认配置。RMON（Remote Monitoring，远程网络监视）完全基于 SNMP 体系结构，用于监视和管理远程网络设备。历史组是 RMON 的一个组，利用 RMON 的历史采样控制功能，交换机会周期性地收集网络统计信息，从而监视网络的使用情况。

命令

snmp-rmon history sample-cfg {*index*} {*port*} {*interval*}

no snmp-rmon history sample-cfg {*index*}

参数

index —— 采样条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

port —— 采样端口，取值范围 1~28。

interval —— 采样间隔，即端口采样的时间间隔，单位为秒，取值范围 10~3600，默认值为 1800。

模式

全局配置模式

示例

配置条目 1-3 的采样端口为 1，采样间隔为 100 秒：

TP-LINK(config)# snmp-rmon history sample-cfg 1-3 1 100

28.8 snmp-rmon history owner

该命令用于配置历史采样条目的创建者，它的 no 命令用于恢复默认配置。

命令

snmp-rmon history owner {*index*} [*owner*]

no snmp-rmon history owner {*index*}

参数

index —— 条目序号，取值范围 1~12，每条命令只能输入一个条目。

owner —— 条目的创建者，可输入 1~16 个字符。缺省时为 minitor。

模式

全局配置模式

示例

配置条目 1 的创建者为 owner1：

TP-LINK(config)# snmp-rmon history owner 1 owner1

28.9 snmp-rmon history enable

该命令用于启用历史采样条目，它的 no 命令用于禁用该条目。

命令

snmp-rmon history enable {*index*}

no snmp-rmon history enable {*index*}

参数

index —— 要启用的采样条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

模式

全局配置模式

示例

启用历史采样条目 1、2、3、4、8：

TP-LINK(config)# snmp-rmon history enable 1-4,8

28.10 snmp-rmon event user

该命令用于配置 SNMP-RMON 事件的用户名，它的 no 命令用于恢复默认配置。事件组是 RMON 的一个组，用来定义事件及其类型，此处定义的事件主要用于在警报配置中触发报警。

命令

snmp-rmon event user {*index*} [*user*]

no snmp-rmon event user {*index*}

参数

index —— 事件条目的序号，取值范围 1~12，每条命令只能输入一个条目。

user —— 事件所属的用户名，可输入 1~16 个字符。缺省时为 public。

模式

全局配置模式

示例

设置条目 1 的用户名为 user1：

TP-LINK(config)# snmp-rmon event user 1 user1

28.11 snmp-rmon event description

该命令用于配置 SNMP-RMON 事件描述，它的 no 命令用于恢复默认配置。

命令

snmp-rmon event description {*index*} {*description*}

no snmp-rmon event description {*index*}

参数

index —— 事件条目的序号，取值范围 1~12，每条命令只能输入一个条目。

description —— 对事件的描述信息，可输入 1~16 个字符，默认为空。

模式

全局配置模式

示例

配置条目 1 的事件描述为 description1：

TP-LINK(config)# snmp-rmon event description 1 description1

28.12 snmp-rmon event type

该命令用于配置 SNMP-RMON 事件类型，它的 no 命令用于恢复默认配置。

命令

snmp-rmon event type {*index*} { none | log | notify | both }

no snmp-rmon event type {*index*}

参数

index —— 事件条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

none | log | notify | both —— 事件类型。选择 none 时，不做任何操作；选择 log 时，交换机将事件记录在日志表中；选择 notify 时，交换机向管理主机发送报警信息；选择 both 时，交换机将事件记录在日志表中并向管理主机发送报警信息。

模式

全局配置模式

示例

配置条目 1、2、3、4、8 的事件类型为 log：

TP-LINK(config)# snmp-rmon event type 1-4,8 log

28.13 snmp-rmon event owner

该命令用于配置 SNMP-RMON 事件的创建者，它的 no 命令用于恢复默认配置。

命令

snmp-rmon event owner {*index*} [*owner*]

no snmp-rmon event owner {*index*}

参数

index —— 条目序号，取值范围 1~12，每条命令只能输入一个条目。

owner —— 条目的创建者，可输入 1~16 个字符。缺省时为 minitor。

模式

全局配置模式

示例

配置条目 1 的创建者为 owner1：

TP-LINK(config)# snmp-rmon event owner 1 owner1

28.14 snmp-rmon event enable

该命令用于启用 SNMP-RMON 事件条目，它的 no 命令用于禁用该条目。

命令

snmp-rmon event enable {*index*}

no snmp-rmon event enable {*index*}

参数

index —— 要启用的事件条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

模式

全局配置模式

示例

启用 SNMP-RMON 事件条目 1、2、3、4、8：

TP-LINK(config)# snmp-rmon event enable 1-4,8

28.15 snmp-rmon alarm config

该命令用于配置 SNMP-RMON 警报管理信息，它的 no 命令用于恢复默认配置。警报组是 RMON 的一个组，警报配置是对指定的警报变量进行监视，一旦计数器超过阈值则触发警报，报警方式将按照事件的类型进行相应的处理。

命令

snmp-rmon alarm config {*index*} [**var** { drop | revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | fragment | jabber | collision | 64 | 65-127 | 128-511 | 512-1023 | 1024-10240 }] [**port** *port*] [**s-type** { absolute | increment }] [**r-hold** *r-hold*] [**r-event** *r-event*] [**f-hold** *f-hold*] [**f-event** *f-event*] [**a-type** { rise | fall | all }] [**interval** *interval*]

no snmp-rmon alarm config {*index*}

参数

index —— 警报管理条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

var —— 计数器，默认选项为 drop。

port —— 端口号，取值范围 1~28。

s-type —— 样例类型，即为警报变量选择取样，并将取样值与阈值进行比较的方法，有

absolute（绝对值）和 increment（增量）两个选项。选择 absolute，则在一个取样周期结束时将取样结果直接与阈值进行比较；选择 increment，则将目前值减去上一次取样值之后的增量与阈值进行比较。默认选项为 absolute。

r-hold —— 触发警报的上升阈值，取值范围 1~65535，默认值为 100。

r-event —— 上升事件，即触发上升阈值警报的事件的序号，取值范围 1~12。

f-hold —— 触发警报的下降阈值，取值范围 1~65535，默认值为 100。

f-event —— 下降事件，即触发下降阈值警报的事件的序号，取值范围 1~12。

a-type —— 警报触发的方式，有 rise（上升）、fall（下降）和 all（全部）三个选项。选择 rise，则只在触发上升阈值后触发警报；选择 fall，则只在触发下降阈值后触发警报；选择 all，则触发上升和下降阈值均触发警报。默认选项为 all。

interval —— 时间间隔，取值范围 10~3600，单位为秒，默认值为 1800。

模式

全局配置模式

示例

设置条目 1，2，3，6 的时间间隔为 1000 秒：

TP-LINK(config)# snmp-rmon alarm config 1-3,6 **interval** 1000

28.16 snmp-rmon alarm owner

该命令用于配置警报管理条目的创建者，它的 no 命令用于恢复默认配置。

命令

snmp-rmon alarm owner {*index*} [*owner*]

no snmp-rmon alarm owner {*index*}

参数

index —— 条目序号，取值范围 1~12，每条命令只能输入一个条目。

owner —— 条目的创建者，可输入 1~16 个字符。缺省时为 minitor。

模式

全局配置模式

示例

设置条目 1 的创建者为 owner1：

TP-LINK(config)# snmp-rmon alarm owner 1 owner1

28.17 snmp-rmon alarm enable

该命令用于启用 SNMP-RMON 警报管理条目，它的 no 命令用于禁用相应的条目。

命令

snmp-rmon alarm enable {*index*}

no snmp-rmon alarm enable {*index*}

参数

index —— 要启用的警报管理条目序号，取值范围 1~12，可输入多条，格式为 1-3,5。

模式

全局配置模式

示例

启用警报管理条目 1、2、3、4、8：

TP-LINK(config)# snmp-rmon alarm enable 1-4,8

28.18 show snmp global-config

该命令用于显示 SNMP 全局配置信息。

命令

show snmp global-config

模式

所有命令模式

示例

显示 SNMP 全局配置信息：

TP-LINK> show snmp global-config

28.19 show snmp view

该命令用于显示视图列表。

命令

show snmp view

模式

所有命令模式

示例

显示视图列表：

```
TP-LINK> show snmp view
```

28.20 show snmp group

该命令用于显示组列表。

命令

show snmp group

模式

所有命令模式

示例

显示组列表：

```
TP-LINK> show snmp group
```

28.21 show snmp user

该命令用于显示用户列表。

命令

show snmp user

模式

所有命令模式

示例

显示用户列表：

```
TP-LINK> show snmp user
```

28.22 show snmp community

该命令用于显示团体列表。

命令

show snmp community

模式

所有命令模式

示例

显示团体列表：

```
TP-LINK> show snmp community
```

28.23 show snmp destination-host

该命令用于显示目的主机列表。

命令

show snmp destination-host

模式

所有命令模式

示例

显示目的主机列表：

```
TP-LINK> show snmp destination-host
```

28.24 show snmp-rmon history

该命令用于显示历史采样条目的配置信息。

命令

show snmp-rmon history [*index*]

参数

index —— 要显示配置信息的采样条目序号，取值范围 1~12，每条命令只能输入一个条目。缺省时显示所有历史采样条目的配置信息。

模式

所有命令模式

示例

显示所有历史采样条目的配置信息：

```
TP-LINK> show snmp-rmon history
```

28.25 show snmp-rmon event

该命令用于显示 SNMP-RMON 事件配置信息。

命令

show snmp-rmon event [*index*]

参数

index —— 要显示事件配置信息的条目序号，取值范围 1~12，每条命令只能输入一个条

目。缺省时显示所有条目的事件配置信息。

模式

所有命令模式

示例

显示条目 2 的事件配置信息：

TP-LINK> show snmp-rmon event 2

28.26 show snmp-rmon alarm

该命令用于显示警报管理条目的配置信息。

命令

show snmp-rmon alarm [*index*]

参数

index —— 要显示配置信息的警报管理条目序号，取值范围 1~12，每条命令只能输入一个条目。缺省时显示所有警报管理条目的配置信息。

模式

所有命令模式

示例

显示所有警报管理条目的配置信息：

TP-LINK> show snmp-rmon alarm

第29章 集群配置命令

集群管理解决了大量分散网络设备的集中管理问题，只需将集群中的一个设备配置为命令交换机，即可通过该命令交换机对集群中的其他设备进行管理和维护。

29.1 cluster ndp

该命令用于拓补发现全局配置，它的no命令用于恢复默认配置。NDP（Neighbor Discovery Protocol，邻居发现协议）用于交换机发现与其直接相连的邻居交换机的信息，为集群的建立提供支持。运行NDP的交换机周期性地向邻居发送NDP报文，NDP报文包含本设备的信息以及NDP信息在接收设备上的老化时间，同时也会接收但不转发邻居设备发送的 NDP 报文。本命令用来设置交换机的NDP相关属性。

命令

cluster ndp [**status** { disable | enable }] [**aging-timer** *aging-timer*] [**hello-timer** *hello-timer*]

no cluster ndp

参数

status —— 是否启用全局NDP功能，缺省时为启用（enable）。

aging-timer —— 老化定时器，即本交换机发送的NDP报文在接收设备上的老化时间。取值范围5~255（秒），缺省时为180。

hello-timer —— Hello定时器，即NDP报文发送的时间间隔。取值范围5~254（秒），缺省时为60。

模式

全局配置模式

示例

开启全局NDP功能，并设置老化定时器为120秒，Hello定时器为50秒：

```
TP-LINK(config)# cluster ndp status enable aging-timer 120 hello-timer 50
```

29.2 cluster ntdp

该命令用于拓补收集全局配置，它的 no 命令用于恢复默认配置。NTDP（Neighbor Topology Discovery Protocol，邻居拓扑发现协议）用来在一定网络范围内收集每个设备的信息以及设备间的连接信息。NTDP为命令交换机提供可加入集群的设备信息，收集指定跳数内的设备的拓扑信息。

命令

cluster ntdp [**status** { disable | enable }] [**interval** *interval*] [**hop** *hop*] [**hop-delay** *hop-delay*] [**port-delay** *port-delay*]

no cluster ntdp

参数

status —— 是否启用全局 NTDP 功能，缺省时为启用（enable）。

interval —— 拓补收集间隔时间，即本交换机拓扑信息收集的周期。取值范围 0~60（分钟），缺省时为 1。

hop —— 拓补收集跳数，它决定了本交换机拓扑收集的范围。取值范围 1~16，缺省时为 3。

hop-delay —— 请求跳数延迟时间，即本交换机收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。取值范围 1~1000（毫秒），缺省时为 200。

port-delay —— 端口跳数延迟时间，即本交换机在相邻端口间转发拓扑请求报文的延时时间。取值范围 1~100（毫秒），缺省时为 20。

模式

全局配置模式

示例

开启全局 NTDP 功能，并设置拓扑收集间隔时间为 20 分钟，拓扑收集跳数为 5，请求跳数延迟时间为 300 毫秒，端口跳数延迟时间为 50 毫秒：

TP-LINK(config)# cluster ntdp interval 20 **hop** 5 **hop-delay** 300 **port-delay** 50

29.3 cluster explore

该命令用于手动启动拓扑信息收集功能。

命令

cluster explore

模式

全局配置模式

示例

手动启动拓扑信息收集功能：

TP-LINK(config)# cluster explore

29.4 cluster

该命令用于集群端口配置，它的 no 命令用于恢复默认配置。

命令

cluster [**ndp** { disable | enable }] [**ntdp** { disable | enable }]

no cluster

参数

ndp —— 端口是否启用 NDP 功能，缺省时为启用（enable）。

ntdp —— 端口是否启用 NTDP 功能，缺省时为启用（enable）。

模式

接口配置模式（interface ethernet / interface range ehternet）

示例

启用端口 5 的 NDP 和 NTDP 功能：

```
TP-LINK(config)# interface ethernet 5
TP-LINK(config-if)# cluster ndp enable ntdp enable
```

29.5 cluster create

该命令用于将当前交换机设为命令交换机，创建集群。命令交换机需要为集群成员动态分配一个在集群内使用的 IP 地址，用于集群内部的通信，以实现命令交换机对成员交换机的管理和维护。

命令

cluster create {*name*} {*ip*} {*ip-mask*}

参数

name —— 集群名称，可输入 1~16 个字符。

ip —— 集群 IP 地址池。

ip-mask —— 集群 IP 地址掩码。

模式

全局配置模式

示例

设置当前交换机为命令交换机，创建集群 c1，并设置集群 IP 地址池为 10.90.90.1~10.90.90.254：

```
TP-LINK(config)# cluster create c1 10.90.90.10 255.255.255.0
```

29.6 cluster manage config

该命令用于集群配置。

命令

cluster manage config {*name*} {*keep-time*} {*interval*}

参数

name —— 要配置的集群名称。

keep-time —— 保持时间，即集群信息在命令交换机中保存的时间。取值范围为 1~255（秒），缺省时为 20。

interval —— 时间间隔，即命令交换机与成员交换机握手报文的时间间隔。取值范围为 1~255（秒），缺省时为 20。

模式

全局配置模式

示例

设置集群 c1 的保持时间和时间间隔为 50 秒：

TP-LINK(config)# cluster manage config c1 50 50

29.7 cluster manage member-add

该命令用于添加成员交换机，它的 no 命令用于删除对应成员。集群成员的加入/删除操作必须在命令交换机上进行。

命令

cluster manage member-add {*member-mac*}

no cluster manage member-add {*member-mac*}

参数

member-mac —— 要加入集群的成员交换机的 MAC 地址。

模式

全局配置模式

示例

将 MAC 地址为 00:74:5D:61:67:48 的交换机添加到集群中：

TP-LINK(config)# cluster manage member-add 00:74:5D:61:67:48

29.8 cluster manage role-change

该命令用于转换交换机的角色。在集群中各交换机所处的地位和功能不同，从而形成了不同的角色，用户可根据自己的需要指定交换机的角色。命令交换机用于配置并管理集群；成员交换机是集群中被管理的设备；候选交换机为可以被命令交换机发现但尚未加入集群的设备；独立交换机是未启用

集群功能的设备。

命令

cluster manage role-change { candidate | individual }

参数

candidate | individual —— 目的角色，分别为候选交换机（candidate）和独立交换机（individual）。可转换的角色与当前交换机角色有关，命令交换机、候选交换机和独立交换机之间的转换关系为：命令交换机⇔候选交换机⇔独立交换机。命令交换机的创建见**cluster create**。

模式

全局配置模式

示例

将当前交换机的角色转换为候选交换机：

TP-LINK(config)# cluster manage role-change candidate

29.9 show cluster ndp global

该命令用于显示拓补发现全局配置信息。

命令

show cluster ndp global

模式

所有命令模式

示例

用于显示拓补发现全局配置信息：

TP-LINK> show cluster ndp global

29.10 show cluster ndp port-status

该命令用于显示指定端口的拓补发现配置状况。

命令

show cluster ndp port-status [*port*]

参数

port —— 要显示拓补发现配置状况的端口号，取值范围 1~28，缺省时显示所有端口的拓补发现配置状况。

模式

所有命令模式

示例

显示端口 2 的拓补发现配置状况：

TP-LINK> show cluster ndp port-status 2

29.11 show cluster neighbour

该命令用于显示集群邻居信息。

命令

show cluster neighbour

模式

所有命令模式

示例

显示集群邻居信息：

TP-LINK> show cluster neighbour

29.12 show cluster ntdp global

该命令用于显示拓补收集全局配置信息。

命令

show cluster ntdp global

模式

所有命令模式

示例

显示拓补收集全局配置信息：

TP-LINK> show cluster ntdp global

29.13 show cluster ntdp port-status

该命令用于显示指定端口的拓补收集配置状况。

命令

show cluster ntdp port-status [*port*]

参数

port —— 要显示拓补收集配置状况的端口号，取值范围 1~28，缺省时显示所有端口的

拓补收集配置状况。

模式

所有命令模式

示例

显示端口 2 的拓补收集配置状况：

```
TP-LINK> show cluster ntdp port-status 2
```

29.14 show cluster ntdp device

该命令用于显示拓补收集设备信息列表。

命令

show cluster ntdp device

模式

所有命令模式

示例

显示拓补收集设备信息列表：

```
TP-LINK> show cluster ntdp device
```

29.15 show cluster manage config

该命令用于显示集群管理的全局配置信息。

命令

show cluster manage config

模式

所有命令模式

示例

显示集群管理全局配置信息：

```
TP-LINK> show cluster manage config
```

29.16 show cluster manage member

该命令用于显示成员信息。

命令

show cluster manage member

模式

所有命令模式

示例

显示成员信息：

```
TP-LINK> show cluster manage member
```

深圳市普联技术有限公司
TP-LINK TECHNOLOGIES CO., LTD.
技术支持热线：400-8863-400
公司地址：深圳市南山区西丽镇红花岭工业区二区7栋
技术支持E-mail：fae@tp-link.com.cn
http://www.tp-link.com.cn